Ref. 5 (machine translation)

Jpn. Pat. Appln. KOKAI Publication 2001-016255

SP Number : A0006P3167

(English Documments Translated by Translation Software)

(54) INTER-NETWORK COMMUNICATION METHOD AND SYSTEM

(57)Abstract:

A

	閉域網 A	閉域網 B	リーバ網ネットワーク
ホスト1	アドレス1	—	アドレス101
ホスト2	アドレス2	—	アドレス220
ホスト3	アドレス3	—	アドレス102
ホスト4		アドレス11	アドレス301 (予約)
ホスト5	—	アドレス22	アドレス321
Server	アドレス100	アドレス [illegible]	アドレス1

B

	閉域網 A	閉域網 B
割り当て区間	アドレス空間 01-300	アドレス空間 301-350
PPP回線1	アドレス空間 101-200	アドレス空間 311-350
PPP回線2	アドレス空間 201-250	アドレス 301
動的割り当て	アドレス空間 251-300	—

PROBLEM TO BE SOLVED: To operate physically one server as if each closed area network had a server in the communication between a plurality of the closed area networks and a server side network.

SOLUTION: In this communication method, when an access server AS has a point-to-point protocol PPP connection request from a terminal in a closed area network to a server, which PPP line in which closed area network is identified, a corresponding line is selected in an address space (Figure B) at a server side assigned in advance by PPP lines of closed area networks, an address of a terminal of the closed area network is made to correspond to the selected line (Figure A), address conversion is applied to a packet and the packet is sent to the server side network. The packet from the server side network is address converted by referring to the Figure A, which PPP line in which closed area network is recognized and the packet is sent to the line.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]In a method of communicating by connecting each of two or more user side networks, and the server side network using PPP (Point-to-Point Protocol), At the time of PPP connection establishment, attest an user side network to which the PPP circuit belongs, and in the server side network. . It can set to two or more address spaces beforehand assigned for every user side network, respectively. To an address chosen from an address space to a network and a PPP circuit which attested [above-mentioned]. Change an address of a packet from a PPP circuit of the user side network, send the packet to the server side network, and And the conversion address and an address before conversion, A conversion table with an user side network and a PPP circuit which were attested is memorized, An internetwork correspondence procedure sending an address of a packet from the server side network to a PPP circuit of an user side network which performs inverse transformation of the above-mentioned address translation, and corresponds with reference to the above-mentioned conversion table.

[Claim 2]The internetwork correspondence procedure according to claim 1 changing a destination address of a packet from the above-mentioned user side network into an applicable address in the server side network in the case of the above-mentioned address translation.

[Claim 3]The internetwork correspondence procedure according to claim 1 or 2 changing a port number to a server of a packet from the above-mentioned user side network into a port number peculiar to the user side network in the case of the above-mentioned address translation.

[Claim 4]The internetwork correspondence procedure according to any one of claims 1

to 3 performing selection of the above-mentioned address dynamically or statically according to a utilization course of an user side network.

[Claim 5]The internetwork correspondence procedure according to any one of claims 1 to 4 carrying out address translation of the packet from the PPP circuit with reference to the above-mentioned conversion table in the address after the above-mentioned PPP connection is established, and transmitting to the server side network.

[Claim 6]In a method of communicating by connecting each of two or more user side networks, and the server side network using PPP (Point-to-Point Protocol), At the time of PPP connection establishment, an user side network to which the PPP circuit belongs is attested, Information which identifies VLAN used when using VLAN (VirtualLAN) beforehand assigned for every PPP circuit of each user side network, Add to a packet from a PPP circuit of an user side network attested [above-mentioned], and it sends to the server side network, An internetwork correspondence procedure sending the packet to a PPP circuit of an user side network for which it asked from information which identifies VLAN of a packet from the server side network.

[Claim 7]In a method of communicating by connecting each of the multiple user side network, and the server side network using PPP (Point-to-Point Protocol), At the time of PPP connection establishment, an user side network to which the PPP circuit belongs is attested, Information which identifies VLAN used when using VLAN (Virtual LAN) beforehand assigned for every user side network, Add to a packet from a PPP circuit of an user side network attested [above-mentioned], and it sends to the server side network, And a conversion table of information and a PPP circuit which identify an address and VLAN of the packet is memorized, An internetwork correspondence procedure asking for a PPP circuit with reference to the above-mentioned conversion table from information which identifies VLAN of a packet from the server side network, and an address, and sending the packet to the PPP circuit of an user side network.

[Claim 8]An access server device formed between the server side networks connected by two or more user side networks and PPP (Point-to-Point Protocol), comprising:

An address space quota table which memorizes an address space assigned for every PPP circuit of each user side network.

A means which attests to which PPP circuit of which user side network a terminal to connect belongs.

An address translation means to change an address of a packet from the above-mentioned PPP circuit into one address currently assigned on the above-mentioned address space quota table, and to send the packet to it to a PPP circuit of an user side network attested [above-mentioned] in the server side network.

A conversion address memory measure which memorizes relation between an address by which address translation was carried out [above-mentioned], and an address before conversion, An address inverse transformation means to send the packet to a PPP circuit of an user side network which changes an address of a packet from the server side network with reference to the above-mentioned conversion address memory measure, and corresponds with reference to the above-mentioned table.

[Claim 9]The access server device according to claim 8 provided with a means to carry out address translation of the packet from a PPP circuit of an user side network with reference to the above-mentioned conversion address memory measure with the address, and to send it to the server side network.

[Claim 10]The access server device according to claim 8 or 9, wherein the above-mentioned address translation means is provided with a means to change a destination address of a packet into an address with which the server side network corresponds.

[Claim 11]The access server device according to any one of claims 8 to 10, wherein the above-mentioned address translation means is provided also with a means to change a port number to a server in a packet into a port number peculiar to the user side network.

[Claim 12]An access server device formed between the server side networks connected by two or more user side networks and PPP (Point-to-Point Protocol), comprising:

A VLAN identification information table which memorized a relation with information which identifies VLAN used when using a PPP circuit and VLAN (Virtual LAN) of an user side network.

A means which attests to which user side network the PPP circuit belongs at the time of

PPP connection establishment.

A means to search for information which discriminates corresponding VLAN from a PPP circuit of an user side network attested [above-mentioned] with reference to the above-mentioned table, to add it to a packet from the above-mentioned PPP circuit, and to send it to the server side network.

A means to send a packet from the server side network to a PPP circuit of an user side network corresponding with reference to the above-mentioned table from information which identifies the VLAN.

[Claim 13]An access server device formed between the server side networks connected by two or more user side networks and PPP (Point-to-Point Protocol), comprising:

A VLAN identification information table which memorized a relation with information which identifies VLAN used when using an user side network and VLAN (Virtual LAN).

A means to attest to which user side network the PPP circuit belongs at the time of PPP connection establishment.

A means which searches for information which discriminates corresponding VLAN from the user side network attested [above-mentioned] with reference to the above-mentioned table, is added to a packet from the above-mentioned PPP circuit, and is sent to the server side network.

A means to remember a conversion table of information and the above-mentioned PPP circuit which identify the above-mentioned VLAN to be an address of the above-mentioned packet, A means to send a packet from the server side network to a PPP circuit of an user side network corresponding with reference to the above-mentioned table and the above-mentioned conversion table from information and an address which identify the VLAN.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]Offer of the hosting service (service lent out to each user side network) of several networks which are different in this invention, especially the extranet-oriented shared server which performs communication between closed networks, The information in which the server on these user side networks (closed network) has public services, such as ticket reservation service, is incorporated. Therefore, it is related with an information distribution correspondence procedure including an electronic commerce, such as providing safely the service (the needs of each user side network were embraced) customized per user side network (closed network), and its device.

[0002]

[Description of the Prior Art]The Internet is begun today, and the closed network is built, in order for network use to spread widely, and to hold down the communication cost in a company at a low price and to perform it safely in many companies. In this construction, it curses not only using a dedicated line but using ATM and FR (Frame Relay), and is

carrying out using IP (Internet Protocol) tunneling. When a business manager etc. connect with these closed networks from a place where one has gone, L2TP (Layer2 tunneling Protocol) which is PPP (Point-to-Point Protocol) and its extension is used. Communication between closed networks will increase from now on, the common server used with two or more closed networks is provided, without losing the closed **** of a self-closed network, or the use which customizes public service of ticket reservation service etc. combining the information which the server on each closed network has increases. Although there is the method of preparing the server which provides service on each closed network as a realization method of this, this has a heavy burden of the side which cost starts and prepares a server. Then, although it is one set of a server physically, from each closed network, it seems that a separate server exists respectively and construction of the virtual private server which can provide the customized service for secure (safe) one is considered.

[0003]Now, in construction of closed networks, such as a company, the method of giving a global address dynamically [only when using a local address or connecting with the exteriors, such as the Internet,], and communicating with the exterior because of shortage of the IP address by the rapid spread of network, is taken. however,/especially connected only at the time of necessities, such as a moving terminal, since the same address is not necessarily given at the time of next connection when giving an address dynamically -- when the connection itself is unstable, it is more necessary to give an address statically. In the situation of giving an address dynamically, since the connection establishment from the server side to a specific terminal is difficult, a local address is statically given in many cases at the time of network construction. When the service provision to the closed network currently physically built in this way by one set of a server is considered, (1) The collision of the address space between the closed networks which are making prevention and (2) connection, such as unjust connection through the server side network, and solution of three problems of the connection establishment to the specific terminal which includes a moving terminal from (3) servers are needed.

[0004]The PPP tunneling art represented by construction of this server at L2TP (Layer2 tunneling Protocol) of the existing art, It can be said that it is the art with two useful

kinds of the address translation art represented by NAT (Network Address Translator). First, connection with its own closed network is always attained, without a moving terminal being restrained by PPP tunneling art at time and a place, and use of a closed network is attained as if it existed in the closed network. As shown in drawing 22, the closed networks A and B are made possible [the server side network and connection] via the Internet/public network, The address in each local address space A and B is given to the host (it is also called a terminal) belonging to each closed networks A and B, Through the access server between nets of the closed network with which it belongs (AS), each host connects with the access server between nets of the server side network using PPP tunneling, and a server and connection of him are enabled. By this composition, by carrying out tunneling of the PPP connection to the server side, as it has connected with the server belonging to its own closed network, it can be shown as a terminal. It becomes possible for this to maintain closed **** which a closed network has, or to use the local address currently assigned with the closed network as it is. However, since a local address is freely assigned to a terminal in (1) closed network, the case where the terminal belonging to several different closed networks has the same address arises, and a collision is not avoided in this case. Therefore, if it sees from the server side network of a connection destination, it will occur that two or more terminals with the same address exist, and it cannot be recognized correctly with which terminal it is communicating at this time.

[0005](2) It is necessary to carry out the address which shows a server in common with each closed network, and the large change to the existing equipment may be needed. (3) When an address is dynamically assigned from the server side at the time of the connection establishment from a terminal, Which address is assigned to the terminal connected to a network if needed like a moving terminal, or are unknown, There is a problem that there is possibility of unlawful access generating over the closed region side, via the network by the side of (4) servers which cannot provide service called the distribute information from the server side which is useful service, and no solution of technical problems can be performed.

[0006]In order for the user terminal given the local address linked to a closed network to

perform communication with the server to which the global address on the Internet was given, the user terminal itself needs to have a global address. However, as mentioned above, since global addresses run short, they are assigning the local address statically to the terminal in many cases. By NAT (network address translation) art, at this time, as shown in drawing 23, perform communication in a closed network using a local address, and for communication with the WWW server on the Internet. It communicates possible by assigning the global address pooled beforehand dynamically to the device which can use NAT provided in the boundary between nets. However, in order that this NAT may make connection between hosts (terminal) from a local address, a global address, and correspondence ****** / address by the group of a port number dynamically, Since the connection between a host and a server is recognized dynamically, service of push types (with no connection establishment demand from a terminal), such as distribute information from the server side with the global address to the terminal which assigned the local address once connection cuts statically, (1) An impossibility, (2) Since a server cannot attest every closed network (discernment), Since providing the service everywhere customized for every group terminal and information has connected the portions of difficulty and (3) NAT to a global address space, there is a problem of the possibility of unlawful access, and no solution of the problems in server construction can be performed.

[0007]To what is considered that the NAT art itself is available to the construction of a server which it is extended and used in various forms and is made into the technical problem on these specifications. There are NAT art which cooperated with PPP, and NAT art by Cisco which can change the both sides of the source address of a packet and a destination address by setting out. In NAT which cooperated with PPP, an NAT function is performed in communication with global IP networks, such as the external Internet, via a PPP circuit using the global IP address began to wave from a server after establishing PPP connection between servers. That is, NAT of the established PPP circuit unit is possible. Construction of the server of a technical problem is considered using this art. If this art is introduced into the device by the side of a server, since NAT can be performed for every PPP circuit, it can perform easily customizing the service used per closed

network, or changing the server to be used in each closed network unit. However, considering realization by one set of a server, there is the following problem.

[0008]

[Problem(s) to be Solved by the Invention](1) Since the closed network of the user equivalent to a client and the network by the side of a server are connected by PPP connection, in connection of the closed networks built by the local address, the collision of an address space will arise like the case where PPP tunneling art is used. The server which received the packet which arrived from the host of the closed network equivalent to a client when this art was especially introduced into the server side, It cannot be identified whether the packet came from the host of which closed network by duplication of the address part which shows the host of a closed network, and a packet cannot be sent out to a surely applicable host.

[0009](2) Since the address which two or more servers by the side of a server have to the address since NAT is performed to the address began to wave at the time of PPP connection establishment is mapped, connection with a specific server is unestablishable among two or more servers [host / of a user's closed network]. In order to be established, a PPP circuit is established according to the number of servers to use, and it is needed to make one address of a server correspond to the address on which PPP decides.

[0010](3) Although it changes to the address which shows a server, if the address after conversion becomes the same as that of the address which shows the host of a closed network, it cannot communicate correctly. Therefore, it is necessary to make it the address which the host of each closed network uses, and the address of the server of the server side network not lap, and investigates what kind of local address is used with each closed network, and in order to decide the address of the server side network, it takes great time and effort and time.

[0011]The NAT art which the said problem cannot be and solve and which Cisco developed, Unlike NAT defined by RFC1631, to the target both sides of the source address of a packet, and a destination address, address translation is possible and using the address translation table by static/dynamic assignment of an address Cooperation

with the application layer, The flexible operation which creates the address translation table used for NAT especially by cooperation with DNS (Domain Name System) is possible. According to such a feature, connection establishment to the host on the closed network built by the local address connected behind the NAT device from the server on the Internet with the difficult global address, etc. is also made possible with the conventional NAT art. Closed **** which a closed network has by canceling a packet when there is no address which shows the host of the exterior of a packet who received in an address conversion table, or restricting the address notified to an external network etc. can also be maintained. If the server considered on these specifications using this art is built, in order that in the case of the closed network built by the local address the (1) server side network may also avoid the collision of an address space and may communicate with the host besides closed networks, such as a server on the Internet, both networks will perform NAT. At this time, since the host of a connection destination cannot be specified unless the global address used for communicating between closed networks at NAT and the local address which a host has are made at least 1 to 1 correspondence, it is useless for communication being impossible. In this case, it not only cannot perform connection with the host of a closed network from the server side, but when two or more servers exist, it cannot perform connection with a specific server for the above-mentioned reason.

[0012]There is a said problem and all cannot be solved. Thus, when the existing art is used, all the problems produced in the server construction described on these specifications cannot be solved.

[0013]

[Means for Solving the Problem]Two or more user side networks (an user side network is henceforth explained as a closed network) which a user uses also in the 1st invention of the 1st invention and the 2nd invention make connection by PPP (Point-to-Point Protocol) to a network by the side of a server. Connection origin which has performed PPP connection in attestation at the time of this PPP connection establishment in addition to the conventional user's attestation attests which PPP circuit of which closed network. According to the 1st invention, by the result, connected PPP connection

matches with each PPP circuit information which shows which PPP circuit of which closed network it is. And an address of the server side network assigned to a PPP circuit applicable as a key in this information, A port number according to service of a server which was decided per closed network if needed and to be used is used, A port number is changed both [a network address and if needed] for sauce and a destination to a packet left from / which comes into the server side network through a PPP circuit.

[0014]In this 1st invention, in the server side network, an address space is uniquely assigned to each closed network unit, and flexible use by a plan of that closed network unit is performed. An address space prepared for each closed network in the server side network is assigned by the following plan. An address space is first assigned statically per PPP circuit. This address space is made to assign per subnet. The amount of static assignment may not be. In that case, all are dynamically assigned to a PPP circuit per subnet. And it shall assign dynamically a PPP circuit using LCP (setting protocol) of PPP, etc. to a PPP circuit which has consumed an address space assigned when there was space which remained. Dynamically, a part for necessity may be sufficient as a size of an address space assigned dynamically, it may determine a fixed size by a negotiation, and can choose it as freedom, such as enlarging a size gradually with a certain algorithm. When a PPP circuit is assigned dynamically, a packet to a terminal by the side of [the server side to] a closed network can be sent out to a suitable PPP circuit by managing which address space was assigned to which PPP circuit of the closed network.

[0015]Thus, since operations including assignment are independently required per closed network, evasion of a problem by collision of an address space of a closed network to connect and connection with a specific terminal are enabled. By the closed network side closed **** which conversion of an address is performed by the server side, control about connection can be easily performed in the server side, and each closed network has is not only maintainable, but connected. It is possible to give an address to a server used freely from an address space of a self-closed network, and a setting variation of a network by which it is accompanied at the time of introduction can be suppressed to the minimum. Hereafter, this address conversion method is called route side NAT (the following, Root-side NAT, or RNAT).

A user's closed network with which the circuit belongs like the 1st invention of the 2nd invention at the time of PPP connection establishment attests either. And information which identifies VLAN used when it uses sufficient VLAN (Virtual LAN) for which PPP circuit of which closed network it is to be discriminable for a PPP circuit, after ending attestation of a closed network of affiliation at the time of PPP connection establishment is matched. And a packet from that PPP circuit is carried to a server to be used with VLAN constructing technique, such as switching, based on information which identifies this VLAN. And OS which carries out various processing to an information unit which identifies each VLAN in one set of a server is operated, and the above-mentioned server is realized.

[0016]When it matches information which identifies sufficient VLAN to identify a closed network in a PPP circuit, an address of a host of a closed network shown in a PPP circuit which received a packet, and its packet is matched. This matching is carried out to an information unit which identifies VLAN. Thereby, an above-mentioned server can be easily built and used by control of the server side network using information which identifies VLAN, without adding change to a user's network. By an authentication result about this closed network that belongs, a method of assigning information which identifies VLAN which can identify a closed network at least is hereafter called VNAT to an established PPP circuit.

[0017]

[Embodiment of the Invention]the 1st shot ** -- an embodiment is first described about the 1st invention. It is assumed that it is considered as the system configuration shown in drawing 1 now. That is, the closed network A, B, and C is connected with the Internet/public network via access server AS, respectively, and the server side network is connected with the Internet/public network via access server R-NAT with a Root-side NAT function by this invention. The address is assigned as the closed networks A and B are shown in drawing 2 A to each host (terminal). That is, in the address space which the closed network A has, it is assumed to the address 1 and the host 2 that the address 100 is assigned to the address 2 and the host 3 at the address 3 and Server to be used at the host 1. Server is one of the hosts who have set to the network by the side of a server,

and, as for this Server, the address 1 is given in the network by the side of a server. As the network by the side of a server is shown in drawing 2 B, the respectively peculiar address space is prepared to the closed networks A and B. The address groups 101-300 are prepared for the terminals connected from the closed network A, The address groups 201-250 are assigned to the terminals which connect the address groups 101-200 to the terminals connected before long from the PPP circuit 1 which the host 1 and the host 3 use from the PPP circuit 2 which the host 2 uses, respectively. And the remaining address groups 251-300 are dynamically assigned if needed to the PPP circuits 1 and 2, when the above-mentioned assignment is used up. In the address space which the closed network B has, the address 150 is respectively assigned to the address 11 and the host 5 at the address 22 and Server to be used at the host 4. The address groups 301-350 are prepared for the terminals connected from the closed network B in the network by the side of a server, and the terminal of the closed network B is statically assigned before long to the PPP circuit established directly to the address groups 301-310. 311-350 shall be assigned to the PPP circuit 1, and shall assign the host using this PPP circuit dynamically at the time of server connection. Thus, an address space is pooled in each closed network unit in the network by the side of a server, an address space is assigned to a PPP circuit according to the utilization course of a closed network, and the host using a PPP circuit further applicable from there is flexibly assigned including static and ****.

[0018]PPP connection of between access server AS set to each closed network and device R-NAT with the function of Root-side NAT is carried out. The terminal of a closed network performs the device (R-NAT) with a Root-side NAT function and PPP connection which used the server using this PPP connection, or were directly set to the server side using PPP tunneling, and uses a server.

[0019]Then, it is this Root-side NAT that is made available in two or more closed networks without showing one set of a server virtually physically on the network by the side of a server so that it may exist in each closed network respectively, and losing the closed **** of each closed network. This Root-side NAT is faced assigning the address prepared beforehand for every closed network by the server side, It is attested to which

PPP circuit of which closed network not only the conventional attestation about the host that it is whether the terminal which is demanding connection at the time of PPP connection establishment with a closed network is the right but the terminal to connect belongs. An address is dynamically assigned to a terminal from the address space prepared per PPP circuit in the thing applicable when the address is statically assigned by the terminal based on this result out of the address group beforehand prepared for the PPP circuit of that closed network when that was not right.

[0020]In drawing 1, when the host 1 has connected and the PPP circuit has not been established yet, establishment of a PPP circuit begins from used AS (access server), and it attests that this PPP circuit is the PPP circuit 1 from the closed network A at this time. And an address is dynamically assigned to a host from the address space pooled for the PPP circuits 1 of this closed network A. Since in this case the address space 101-200 is given to the PPP circuit 1 as shown in drawing 2 B, and it gives dynamically from this space, the address 101 which is not used is assigned to the host 1 in the server side network. That is, the address 1 given by RNAT with the closed network A about the packet from the PPP circuit 1 of the closed network A will be changed into the address 101. As this relation shows drawing 2 A, it memorizes as a table. Then, if a packet comes from the host 1 through the PPP circuit 1 of the closed network A, with reference to the table of drawing 2 A, it will be changed into the address 101 of the server side network by the address 1. Similarly, when the packet from the host 3 comes, the address 102 which is not used is dynamically assigned to the host 3 from the same address space because it is from the PPP circuit 1, and the address 3 which the host 3 has by RNAT is changed into the address 102. Since the PPP circuit 2 which is another PPP circuit is used when the host 2 connects with a server, It will assign from the address space 201-250 prepared for the PPP circuits 2, the address 220 which is not used is assigned in the network by the side of a server, and the address 2 is changed into the address 220 by RNAT.

[0021]The host 4 is doing PPP connection to the device by the side of a server directly using PPP tunneling, establishment of a PPP circuit starts, and it is attested by the same attestation at this time that this PPP circuit is the PPP circuit 2 from the closed

network B. And since the address 301 is statically assigned to the PPP circuit 2 of this closed network B, the address 11 which the host 4 has by RNAT will be changed into the address 301 in the server side network. When the host 5 connects with a server, it is attested that the PPP circuit to be used is the PPP circuit 1 of the closed network B, and the address which is not used from the address space 311-350 prepared for the PPP circuit 1 is dynamically assigned to the host 5. This time, the address 311 is assigned. The packet to a server is changed into the address 311 from the host 5 to the address 22 which the host 5 has by RNAT.

[0022]Conversion to the address which also assigned the address of Server specified as the connection destination to Server in the network by the side of a server is performed. This time, about the closed network A, the address 150 of Server will be changed into the address 1 for the address 100 of Server to the address 1 about the closed network B. Although restriction of the service based on the address assigned per closed network to be used is also possible, service provision of a closed network unit is physically made possible by one set of a server with the port number of a server by deciding the port number of the server used per closed network. This time, the service closed-network A Turned in Server is port number A, and suppose that the service to closed-network B Turn is provided by port number B.

[0023]Root-side NAT performs the sauce of a packet, the network address of both destination, and conversion of a port number under management by the side of a server based on matching and the port number of this address. When the host 1 uses WWW Server (port number 80) of Server, conversion operation as shows drawing 3 the host's 1 packet by RNAT will actually be performed. Drawing 3 A shows the packet from the host 1 to a server, and drawing 3 B shows conversion by each R-NAT of the packet from a server to the host 1.

[0024]That is, when the address translation portion in Root-side NAT is summarized, it comes to be shown in drawing 4. In this figure, the address group by which NetA was prepared for the address group of the network with which Server exists in the address space of the network by the side of a server, and each closed networks [in / in NetB / the address space of the network by the side of a server] is summarized. The address

group prepared for each closed networks as shown in drawing 5 A terminal. Or it is statically assigned to each PPP circuit linked to a network, and when the space currently assigned statically stops being sufficient, the remaining space is used in order to assign dynamically according to a demand to the PPP circuit which run short. A packet can be sent out to a suitable PPP circuit by managing which PPP circuit the space assigned dynamically was assigned at the time of assignment. Thus, the space prepared for the server side network can choose the plan of use of the closed network which is a user of each space. Matching the address of the terminal in each closed network with the address beforehand prepared for the server side for every closed network respectively Compaction (Compaction) conversion, It carries out changing into the address of the server in the network by the side of a server the address of Server assigned in each closed network to calling it merge (Merge) conversion. Reverse Compaction conversion is discriminated from the address assigned by the terminal with reference to drawing 2 A and B for which PPP circuit of which closed network it is, and is changed into the address of the terminal in the closed network. Reverse Merge conversion changes the address of a server into the address of the server in a closed network from the information on the terminal belonging to which closed network obtained from reverse Compaction conversion with reference to drawing 2 A. And a packet is sent out to the suitable PPP circuit of a suitable closed network by discernment of which PPP circuit of which closed network. At this time, the above-mentioned conversion is performed to the sauce and the destination address of the packet from a terminal to a server, and the packet from a server to a terminal, as shown in drawing 6. It changes into the port number used in the closed network from the port number decided per closed network in the server side network also about the port number of the used server.

[0025]The address space given for every closed network of this, Since it assigns as a result of the attestation about the closed network which belongs, since it is attested, which closed network each address is is forbidding connection between the addresses of this different closed network by the server side, it will forbid communication between closed networks as a result, and can secure closed **** which a closed network has. It becomes possible to customize the service provided by carrying out based on this

address space assigned to each closed network, or deciding the port number which can be used in a server to each closed network for every closed network. The feature of conventional technology and the 1st invention (route side NAT) is summarized to drawing 7, and is shown.

The system configuration to which the 2nd invention of the 2nd invention is applied is shown in drawing 8. The closed networks A and B are connected with the Internet/public network via access server A5, respectively, and the server side network is connected with the Internet/public network via the access server VNAT with a VNAT function. In the access server VNAT with a VNAT function, as shown in drawing 9, a VLAN tag is assigned to each PPP circuit of each closed network. Hereafter, change by this assignment is called VNAT. Access server AS set to each closed network performs PPP connection to the access server VNAT with the VNAT function which the server side network has.

[0026]VLAN1-x is assigned as the information which identifies VLAN used when they use VLAN which shows the closed network A, since the hosts 1, 2, and 3 are all hosts of the closed network A, for example, a VLAN tag. Next, in order to identify two or more PPP circuits from the same closed network, the child number x is assigned. The hosts 1 and 3 are coming from the same PPP circuit 1, and VLAN1-1 is matched with the PPP circuit 1 as a VLAN tag. Since the host 2 has connected using the PPP circuit 2 of the closed network A, he is matched with the PPP circuit 2 to which VLAN1-2 corresponds as a VLAN tag. Similarly, since the hosts 4 and 5 are hosts belonging to the closed network B, VLAN2-x will be assigned as a VLAN tag in which the closed network B is shown. In order to identify a PPP circuit like the case of the closed network A, VLAN2-2 is assigned to the host 4 and VLAN2-1 is assigned to the host 5.

[0027]This VLAN tag is embedded at the packet received from the closed network based on assignment of a VLAN tag in the device VNAT which has a VNAT function as shown in drawing 10. And this packet is carried by the existing VLAN art, such as IEEE802.10 and a switching function of VLAN correspondence, based on this VLAN tag to Server. As shown in drawing 11, in order to perform separate processing for every VLAN tag, Server which receives a packet is changed so that two or more OS's can operate, and it is made

for one OS to operate to the VLAN tag of the unit which can identify a closed network. That is, two or more OS's are made to operate in one machine in the condition said in OS2 for performing processing about OS1 for performing processing about the tag of VLAN1-x, and the tag of VLAN2-x. In the network by the side of a server, since delivery of a packet is performed based on a VLAN tag and virtual closed networks including the server on the network by the side of a server can be built, it is not necessary to change at all by the server side about the address of a packet. Thus, a virtual private server can be built, without losing closed **** which a closed network has under management by the side of a server in operating OS for every VLAN tag in one set of a server.

The modification of the 2nd invention of modification of the 2nd invention is shown below. Since the hosts 1, 2, and 3 are all hosts of the closed network A, VLAN1 is assigned as a VLAN tag in which the closed network A is shown. Next, when two or more PPP circuits from the same closed network are established, the address and PPP circuit which show a host are matched so that the packet addressed to the host can be returned to the PPP circuit which received the packet. The hosts 1 and 3 are coming from the same PPP circuit 1, and each address is matched with the PPP circuit 1. Since the host 2 has connected using the PPP circuit 2 of the closed network A, VLAN1 is assigned as a VLAN tag, but the host's 2 address 2 is matched with the PPP circuit 2.

[0028]Similarly, since the hosts 4 and 5 are hosts belonging to the closed network B, VLAN2 will be assigned as a VLAN tag in which the closed network B is shown. In order to return a packet to the PPP circuit similarly thought to be a case of the closed network A, a host's address and PPP circuit are matched. In this case, the host's 5 address is matched with the PPP circuit 2 for the host's 4 address by the PPP circuit 1. since matching of the address of this PPP circuit and a host is performed per VLAN tag as shown in drawing 12 -- VLAN1 and VLAN2 -- matching is performed independently respectively. By reference, matching about VLAN1 serves as the following. The newest connection times in this matching can also be doubled and managed, and security can also be raised by providing timeout etc. In the device which is performing this VNAT conversion if the packet from a server is received, The conversion table which uses as a key the VLAN tag currently embedded at the packet, and searches it first is decided, and

the PPP circuit which should search and send out a conversion table is investigated by using as a key the destination address (a host's address) currently embedded next at the packet. The result can send out to the PPP circuit which received the packet.

As an example using the virtual private server which becomes possible by the method of an invention of ********, it states using the example of the procurement service for two or more contractors. In order to act as the company A for supply of the company 1, to carry out a supply request to B respectively and to choose this time the one where either is better, it is an example in the case where it is necessary among companies registration of data, and to exchange and suit.

It is assumed that it is network composition as shown in example drawing 13 of the 1st invention. The closed networks A and B and 1 are connected with the Internet by access server AS1, AS2, and AS3, respectively, An ISDN network is connected with the Internet by access server AS4, and the server side network is connected with the Internet by access server R-NAT with a route side NAT function. As device R-NAT with a route side NAT function is shown in drawing 14, the conversion table of an address is created and it operates. How to make a conversion table is mentioned later. Here, the closed network N shall mean the closed network which the company N has. PPP connection of between device R-NAT with a route side NAT function set to the network of the server network, and access server AS1 placed by each closed network, AS2 and AS3 is carried out using tunneling. It can connect with access server AS4 using ISDN etc., and the host who belongs to a closed network via this can also perform device R-NAT and PPP connection in the direct server side network.

[0029]As shown in drawing 12 from the address space which the closed network which belongs has, the address is respectively assigned to the host of each closed network. In order to use the function of this Root-side NAT, in the network by the side of a server, the address space is pooled for each closed network. In this example, an exhaust air address expresses in the closed network A, the address space of the 10.10.1.0 subnet masks 255.255.255.0 is prepared, and an address is assigned to the terminal connected from the closed network A from this space. Similarly the address space of the 10.10.2.0 subnet masks 255.255.255.0 is prepared for the closed network B, The address space of

the 10.10.11.0 subnet masks 255.255.255.0 is prepared for the closed network 1 from this space at the terminal connected from the closed network B, and an address is assigned to the terminal connected from the closed network 1 from this space.

[0030]In the closed network A, the host 1 presupposes 10.0.1.13 and the host 2 that 10.1.1.1 is assigned to 10.0.3.20 and WWW Server to be used. Actually, WWW Server is set to the network by the side of a server, and this WWW Server provides service in the network by the side of a server to the terminal which 10.100.10.1 is assigned and belongs to several different closed networks. The inside of the address space 10.10.1.0 subnet mask 255.255.255.0 currently assigned to the closed network A in the network by the side of a server, The 10.10.1.0 subnet masks 255.255.255.192 are assigned to the PPP circuit 1, and the 10.10.1.64 subnet masks 255.255.255.192 are assigned to the PPP circuit 2. And in order to assign the space 10.10.1.128 remaining subnet masks 255.255.255.128 to the PPP circuit dynamically demanded per subnetwork according to the demand from the PPP circuits 1 and 2, there are [for]. When the terminal of the closed network A uses WWW Server, it is set up in the network by the side of a server develop the service for closed network A with the port number No. 8080.

[0031]Now, when the host 1 uses WWW Server, the PPP circuit 1 established from the access server 1 (the following, AS1) is used. When the PPP circuit 1 is not established between AS1 and AS with a Root-side NAT function by the side of a server (henceforth, RNAT device), PPP connection is established first. At this time, it is attested which PPP circuit of not only a host's attestation but which closed network it is. In this case, it is attested that it is the PPP circuit 1 of the closed network A. Next, it is confirmed whether there is any address which is not used for the address space currently assigned to the PPP circuits 1 of the closed network A in the server side network. It supposes that there is an address which is not used in this case, and 10.10.1.15 is dynamically assigned to the host 1 from the space. In [when all the space for PPP circuit 1 is already used, AS1 requires the address space of a required part using LCP of PPP, etc., and] a RNAT device according to this, In order [which the closed network A has] to assign dynamically, a part granted a permission will newly be assigned among demands to two or more PPP circuits 1 from the space 10.10.1.128 subnet mask 255.255.255.128 currently

prepared, and an address will be dynamically assigned to the host 1 out of it. At this time, it manages with a RNAT device which PPP circuit the space to assign assigned, and, thereby, a packet can be sent out to a suitable PPP circuit. The amount of [which a required part of the subnet unit was assigned, and also was decided] fixed subnet space may assign dynamically, and it may enlarge subnet space as a unit gradually.

[0032]In the closed network A, an address is 10.0.3.20, and the host 2 connects with a server using the PPP circuit 2 established between ASI and a RNAT device. It is attested like the case where the host 1 connects, at the time of this PPP connection establishment that this PPP circuit is the PPP circuit 2 belonging to the closed network A. And the address which is not used from the space 10.10.1.64 subnet mask 255.255.255.192 prepared for the PPP circuits 2 of the closed network A is searched, and the host 2 is assigned. This time, 10.10.1.100 is dynamically assigned to the host 2. If all the space prepared beforehand is used, an address space will be dynamically assigned to the PPP circuit 2 like the time of being the host 1, and the host 2 will be dynamically assigned from the space. Thus, an address is assigned to the host who has connected in the network by the side of a server, and an address translation table required for a RNAT function is made.

[0033]In a RNAT device, the source address of a packet is changed into 10.10.1.15 from 10.0.1.13, and the case to WWW Server changes a destination address into 10.100.10.1 from the host 1 from 10.1.1.1. In order to use WWW Server, the host 1 advances a utilization request to the port number 80 of a server, but. A port number is also changed into the port number 8080 of the server which provides the service for closed network A in a RNAT device, it is correctly sent to a server by routing of the after-conversion server side network, and use of the service to closed-network A Turn is performed.

[0034]Conversely, the packet from WWW Server to the host 1, His being the host 1 who belongs a destination address to the closed network A from 10.10.1.15, and the thing which are established from AS1 and which is the packets to turn PPP circuit 1 are identified, and an address is changed into 10.0.1.13. Next, the host 1 changes a source address into 10.1.1.1 from the information that it belongs to the closed network A, from 10.100.10.1. And a port number is also changed into the port number 80 specified as the

packet which the host has sent from 8080. A packet is sent out to the PPP circuit 1 of the closed network A which is a suitable PPP circuit using the information based on the destination address which the received packet has after this conversion.

[0035]Similarly, the case of the closed network B is described. In the closed network B, the host 3 presupposes 10.0.1.30 and the host 4 that 10.10.15.1 is assigned to 10.0.1.14 and WWW Server to be used. Actually, WWW Server is set to the network by the side of a server, and 10.100.10.1 is assigned to this WWW Server in the network by the side of a server like the above-mentioned. In the network by the side of a server, the address space currently assigned to the closed network B, Are the 10.10.2.0 subnet masks 255.255.255.0 and in the closed network B. Use in which the terminal itself carries out PPP connection to a RNAT device directly is also performed, therefore, for those reasons, the space of 10.10.2.64. subnet mask 255.255.255.192 is prepared, and the address is statically assigned to each PPP circuit and 1 to 1 correspondence. This time, the PPP circuit 2 or subsequent ones considers it as the PPP circuit established directly from a terminal, 10.10.2.65 is assigned to the PPP circuit 2, and, as for other applicable PPP circuits, one address is assigned statically. The space of the 10.10.2.0 subnet masks 255.255.255.192 is statically assigned to the PPP circuits 1 established from AS2, and an address is dynamically assigned to the host using this PPP circuit from this space. The space 10.10.2.128 remaining subnet masks 255.255.255.128 are prepared in order to assign dynamically according to the demand from the PPP circuit 1 which uses an assigned part.

[0036]Since the host 3 has connected using the PPP circuit 1 established by AS2, If it is attested like the host 1 of the closed network A, or the case of 2 that the used PPP circuit is the PPP circuit 1 of the closed network B, If search and it is [whether there is any address which is not used for the space 10.10.2.0 subnet mask 255.255.255.192 assigned statically, and], arbitrary things will be assigned out of it. This time, 10.10.2.10 is assigned to the host 3 in the server side network. Now, the host 4 is moving, does receipt to nearby AS4, and establishes a PPP circuit directly to a RNAT device using PPP tunneling. At the time of this establishment, it is attested that a PPP circuit is the PPP circuit 2 of the closed network B, and the address 10.10.2.65 with which one

address is statically assigned and the PPP circuit 2 is assigned in this example turns into the host's 4 address. The address of WWW Server is the same as the case of the closed network A. As for the port number which shows the service to be used, the port number 8081 is assigned to the closed network B.

[0037]At the time of the communication to WWW Server (port number 80) from a actual host. The sauce and the destination address which a packet has in a RNAT device by the conversion table etc. which are shown in drawing 14 like the hosts' 1 and 2 case are changed respectively, and it is further changed into No. 8081 specified to the closed network B from 80 about a port number. Conversely, the packet from WWW Server to a host also changes the address and port number of both sauce and a destination which a packet has like the above-mentioned. When two or more PPP circuits exist from which is the closed network to which a host belongs with the destination address of a packet, and its closed network at the time of this conversion, it can be judged to which PPP circuit it sends out. The port number connected to a server based on this information is also changed. And it is sent out after an address and a port number changing in a suitable PPP circuit. For example, in the case of the packet to the host 3, since 10.10.2.10 is given as a destination address, it is identified that it is a packet which this should just send out to the PPP circuit 1 of the closed network B, and it is sent out.

[0038]In the host 5 of the closed network 1, it operates similarly, an address is assigned to the host 5 by the quota plan of the address space which the closed network 1 determined, a table as shown in drawing 13 is made, and address translation is performed about the host 5 using this. If it is the port number 8088 of the server utilization time decided for the closed networks 1, conversion will be performed also about a port number. It is sent to the suitable PPP circuit of a suitable closed network by the same structure as the above-mentioned also to the packet from the server side network to a host.

[0039]the address being guaranteed in the meaning that a closed network is shown, since an address is assigned in the network by the side of a server here as a result of having attested the closed network which belongs, and restricting based on this address -- restriction in a closed network unit -- a line -- it is equivalent to things. That is, WWW

Server with the address 10.100.10.1, By permitting only the connection from each address space of the 10.10.1.0 subnet masks 255.255.255.0, the 10.10.2.0 subnet masks 255.255.255.0, and the 10.10.11.0 subnet masks 255.255.255.0. Restriction can perform easily use from addresses other than this, i.e., other closed networks. Thereby, communication between the limited closed networks can be performed, maintaining closed ****. Not only the access restriction to the data using an address but the port number used per closed network like this time is decided, The program which answers the port number unit at it is operated, and service physically customized for [by one set of a server] two or more closed networks can be realized by setting up the data which can be referred to, the data which can be referred to and changed, etc.

[0040]Even if data is on the same server by distinguishing respectively the data which the program which is operating to the port numbers 8080 and 8081 currently assigned to the closed networks A and B in this case can access, and can be operated, as for the closed network A, the data which he registered can perform reference and change, but. It can prevent changing also from, of course seeing the data which the closed network B registered. On the contrary, the program which is operating to the port number 8088 assigned to the closed network 1, If the program which is operating with the previous port numbers 8080 and 8081 enables it to access both data which can be accessed and operated, respectively, the host of the closed network 1 can refer to the data which both the closed network A and B manage independently. The technical problem that the company 1 of the order Lord demanded in the procurement service made into this example by this can see freely the data of both the company A which is the orderer, and B is cleared. This may restrict with a port number like this time, and may restrict using the address space assigned per closed network. Communication between different closed networks through the network by the side of a server can be prevented by forbidding the communication in a different address space, and closed **** which a closed network has can be maintained. Since the address of the server of a connection destination is also manageable by the server side, if two or more servers are prepared, the load sharing of a server will also become possible by changing an address according to the load of a server.

[0041]Next, the time of communication with the closed network A and the server side network is described for the motion by the DNS (Domain Name System) server which carries out work important at the time of communication by an IP network as an example. In drawing 12, the case where the host who belongs to a user's closed network first connects with the host of the network by the side of a server is described. In order that the host 1 belonging to the closed network A may connect with the WWW server of the server side network, the address of a WWW server to connect to DNS server 2 on the closed network A is asked. Since the address is assigned to the WWW server in the address space of the closed network A, DNS server 2 returns the address 10.1.1.1 assigned to the server applicable with the closed network A to the host 1. And the host 1 sends out the address 10.0.1.13 in which he has a source address, the address 10.1.1.1 in which a server has a destination address, and the packet made into the port number 80 of a destination. And by setting up routing correctly reach AS1 in the packet addressed to 10.1.1.1 in the network of the closed network A, this packet reaches AS1, if necessary, will establish a PPP circuit and will be carried to the device with a RNAT function of the server side network. Based on the conversion table in which self has a destination address of a packet, the device with a RNAT function which received this packet is changed into 10.100.10.1 from 10.1.1.1. Next, 10.0.1.13 of a source address is searched in a conversion table. The address will be used, if an applicable address exists as a result of searching, In the case of this example, it changes into 10.10.1.15, and is further changed into the port number 8080 to which the port number 80 of the destination was assigned for closed network A, and the packet is carried to an applicable server. When there is no applicable address, in the server side network, it is assigned by the above-mentioned method, and communication is performed like the usual case below.

[0042]When the address of the server to connect to DNS server 2 temporarily is not registered, DNS server 2 asks DNS server 1 which is a DNS server of the server side network the address of a server. This inquiry packet is sent to the RNAT device of the server side network via AS1 by routing. The received RNAT device changes both the sauce of a packet, and a destination address based on a conversion table. And when an applicable packet is an address inquiry packet of DNS, change is not added to the data of

a packet but it sends to DNS server 1. DNS server 1 returns the address of the server of the specified connection destination as a response. In this case, the address 10.100.10.1 of a server is embedded as data. This response packet is sent to a RNAT device by routing of the server side network. It identifies that what is necessary is just to send out the received RNAT device to the PPP circuit 1 by which the packet is coming from AS1 of the closed network A from the destination address 10.10.1.62 (address statically assigned to DNS server 1 of the closed network A in the server side network), Sauce and a destination address are correctly changed by conversion about the closed network A. When this packet is a response packet of DNS and it is what returns a host's address, It is changed into 10.1.1.1. which is an address of the server to which the address 10.100.10.1 of the server embedded as data was assigned in the closed network A, and this packet is sent to DNS server 2. DNS server 2 which received this answers to the host 1 as an address of a server to connect 10.1.1.1 to, and the host 1 communicates by sending out a packet like the usual connection.

[0043]Conversely, the case where the WWW server on the server side network connects with the host 1 of a closed network is described. First, the server of the server side network asks DNS server 1 the host's 1 address. Since DNS server 1 does not know the host's 1 address, the host 1 recognizes that he is a host who belongs to the closed network A first from the domain name etc. which are contained in the host's 1 name. And the packet of an address inquiry is sent out by making into a destination address the address (in the case of this 10.10.1.62) assigned in the server side network to DNS server 2 which is a DNS server of the closed network A. In the network by the side of a server, routing of this packet is carried out to a RNAT device. The RNAT device which received the packet discriminates that it is a packet to turn PPP circuit 1 of the closed network A from a destination address, and changes it by the conversion table in which self has both sauce and a destination address to the address space of the closed network A. And it is sent out to DNS server 2 of the closed network A.

[0044]DNS server 2 which received this packet is sent to DNS server 1 of the server side network by making the address 10.0.1.13 in the host's 1 closed network A asked into a response. The RNAT device of the server side network receives this packet, and it

changes sauce and a destination address from a conversion table respectively first. And since this packet is an answer of a host's address inquiry, a host's address part currently embedded to data is changed into the address of the server side network. If there is data which searches the conversion table which a RNAT device has at this time, and corresponds, it will change into an address corresponding from a conversion table, and will send to DNS server 1. When there is no applicable data, the address of the host 1 who is a response from DNS server 2 is changed into the address which assigned and assigned the address dynamically from the address space assigned to the PPP circuits 1 of the closed network A by the above-mentioned method to the host 1, and it sends to DNS server 1. This time, the address 10.10.1.15 will be assigned and changed. At this time, the address information about the host 1 applicable to the conversion table which a RNAT device has is added. Thus, the address of the host who is a response of a DNS server is changed, and is notified to the server which is carrying out the connection request to the host of the closed network with which a translated address corresponds. And by making the notified address into a destination address, a server tries connection with the host belonging to a closed network, the connection with a host from the server side is established by the address conversion function by RNAT, and communication is started.

[0045]Use becomes do not need to add change to the existing DNS server and possible [cooperation with a DNS server is possible by doing in this way, and], introduction in the IP network used for many communications is easy, and establishment of the connection from both directions of the host of a server and a closed network can be realized. If the notice of an address is restricted using a DNS server, fine control, such as limiting the host of the closed network which can perform connection from a server, can also be performed, and maintenance of closed **** by the plan of a closed network can be performed.

[0046]As mentioned above, in the network by the side of a server, prepare an address space for every closed network, and further, Since each portion which determines the port number which can be used to a server for every closed network and to which the received packet to /Send out corresponds is changed, realization of every distribute

information from the server side to a terminal, closed network, or the service customized for every area is attained. Construction of the virtual private server which can perform offer of service by one set of a server to two or more closed networks holding closed **** which a closed network has since the address was furthermore assigned per closed network is enabled. Reuse of the address once assigned dynamically by carrying out the quota term of validity of the address assigned dynamically to to a certain fixed time / existing end of an event is possible, and it is also possible to secure scalability and security.

The case where the company 1 supplies to the companies A and B is made into an example, and is described. [as well as the case of the example of the 1st invention of an example of the 2nd invention] It seems that network composition is shown in drawing 15. That is, the closed networks A and B and 1 are connected with the Internet by access server AS1, AS2, and AS3, respectively, and the server side network is connected with the Internet by the access server with a VNAT function. The closed network N shows the closed network which the company N has. In a device with a VNAT function, a VLAN tag is assigned per PPP circuit of each closed network based on drawing 16. When the host 1 uses the server on the server side network, PPP connection will be established if there is no PPP connection between AS1 and AS with a VNAT function (henceforth, VNAT device). In the attestation at the time of this PPP connection establishment, it is attested that this PPP circuit is the PPP circuit 1 of the closed network A. VLAN1 is assigned as a VNAT tag in which the closed network A is shown, in order to show the PPP circuit 1 until now, a child number is used and a VLAN tag called VNAT1-1 is assigned to this PPP circuit 1. Thereby, it is discriminable that it is the PPP circuit 1 of the closed network A. When the PPP circuit 2 is established, a child number is made to correspond to a PPP circuit like VLAN1-2. what is necessary is just to be able to identify which PPP circuit of which closed network described here as the amount of information using the existing things, such as what defined by IEEE802.10 etc., the form of a VLAN tag is in order to use the existing VLAN art

[0047]About the packet which comes to the network by the side of a server through this PPP circuit with a VNAT function, as shown in drawing 9, a VLAN tag is embedded, and

it is delivered based on this tag to a server. And in a server, it processes by operating separately the program which performs various processings for every VLAN tag, for example, OS. In this server, a suitable VLAN tag can be attached and sent out towards a host at the time of sending out of a packet by associating the information of the host linked to a VLAN tag. Thereby, without needing, conversion of the address in the server side network can use a server as if it existed in the self-closed network. Since the OS is operating for every VLAN tag, it can change now flexibly per closed network, the data referred to and registered can also use a VLAN tag as a key, and the operation can apply restriction. When sent out from the server side network to a closed network, the VLAN tag currently attached to the received packet is removed, a closed network suitable as the address for delivery of a packet and a suitable PPP circuit are discriminated from a VLAN tag, and it sends out to a right PPP circuit.

[0048]Since the PPP circuit 2 is used when the host 2 connects with the network by the side of a server, a VLAN tag will be assigned to the packet from this host 2 to the server side network like the above-mentioned method, and VLAN1-2 will be used. It operates like the host's 1 case using this tag. Although the VLAN tags embedded at each packet differ, since it opts for operation based on VLAN1 which shows the closed network A, even if the server differs in the PPP circuit to be used, it can refer to it for it and change the same data. On the contrary, as for the packet from a server to the hosts 1 and 2, it is identified with a VLAN tag that it is a thing to the closed network A, further, based on the child number of a VLAN tag, the packet to the host 1 can be distributed to the PPP circuit 1, and the packet to the host 2 can be appropriately distributed to the PPP circuit 2.

[0049]Since the hosts 3 and 4 have connected with the server side network via the AS2 [same] and use both the PPP circuits 1, the VLAN tag to be used is the same, using VLAN2-1, is built into a packet in a VNAT device, and is sent to a server. The packet from a server to a host is also sent to a host through a suitable PPP circuit like the above-mentioned host 1.

[0050]VLAN3-1 which is a VLAN tag which the closed network with which it belongs similarly at the time of PPP connection establishment in the host 5 shows VLAN3 which

is a VLAN tag in which it is attested that it is the closed network 1 and this is the PPP circuit 1, and the closed network 1 is shown based on it, and the PPP circuit 1 is assigned. And it sets between servers with a host correctly by the same operation as other hosts, and is carried out. A VLAN tag from OS which carries out processing about VLAN3. The user of the company 1 can see the data which the companies A and B registered by enabling it to refer to the data in which a VLAN tag can refer to only VLAN1 and VLAN2, and communication between closed networks with the restriction which is needed for the procurement service used as this example is realized.

[0051]Next, although it is the motion by the DNS (Domain Name System) server which carries out a motion important at the time of communication by an IP network, In the 2nd invention, surely a server is on the network by the side of a server, but. Since communication within a closed network is virtually realized by use of the VLAN function, The same use as the usual case is possible for a DNS server, and use becomes possible only by setting up so that routing may be carried out correctly to the VNAT device which has surely the packet addressed to an address assigned to the server in the network by the side of a server in a closed network, and AS which can carry out PPP connection.

[0052]Thus, the address of a server is made into a destination address, The packet is carried to the server side network, Offer of service by the virtual private server which can operate as if it makes a change the minimum and users' network had a server respectively to two or more closed networks by the server of one basis of control by the side of a server is attained.

[0053]The example over modification of the 2nd invention is shown below. The closed network which belongs at the time of PPP circuit establishment is attested, and the address of the host who is the sending-out origin of the packet thought to be a PPP circuit is matched per closed network. In this case, a VNAT device will have a table as shown in drawing 17. A VLAN tag, VLAN1, VLAN2, and -- are beforehand assigned to each closed network A and B--.

[0054]If the host 1 tries connection to the server side network, the PPP circuit 1 will be established between AS1 and a VNAT device, and it will be attested that it is the closed network A. And VLAN1 of a VLAN tag is assigned to this PPP circuit 1 by this

authentication result. And when the packet from the host 1 reaches a VNAT device, with a VNAT device, the host's 1 address 10.0.1.13 embedded at the packet and the PPP circuit 1 to which the packet has been carried are matched. And the VLAN tag assigned by the authentication result is embedded and it is sent to a server. On the contrary, if a packet arrives from a server, the thing about VLAN1 will be chosen from the conversion table of drawing 17 by VLAN1 of the embedded VLAN tag, It searches by using as a key the address 10.0.1.13 of the host 1 who is a destination address of a packet, and from a conversion table, it recognizes that what is necessary is just to send out this packet to the PPP circuit 1 established between the closed networks A, a VLAN tag is removed, and it sends out to the PPP circuit 1. Thus, even when two or more PPP circuits are established from the same closed network, a packet can be correctly sent out to the PPP circuit which received the packet.

[0055]Since it is a host belonging to the closed network A in the case of the host 2, VLAN1 is assigned like the host 1. However, since the used PPP circuit differs from the host 1, the host's 2 address 10.0.3.20 is matched with the PPP circuit 2. Although VLAN1 is embedded like the host 1 by this at a packet, as for the packet from a server, the packet addressed to host 2 is appropriately sent by this conversion table using the PPP circuit 2. Also in the hosts 3, 4, and 5, a VLAN tag is assigned by the same method, a host's address and PPP circuit are assigned, and it is independently managed per VLAN tag. Thereby, a packet can be sent out to the suitable PPP circuit of a suitable closed network.

[0056]Next, with reference to drawing 18, the R-NAT device in drawing 1, i.e., the outline functional constitution of an access server with a route side NAT function, is explained. Two or more PPP line processing parts 11 are formed, and the authentication section 12 is attached to the PPP line processing part 11. That attestation which is which PPP circuit of which closed network is checked by the authentication section 12 in the case of PPP circuit establishment, An open address is assigned to the host of a packet who arrived using the PPP circuit with reference to the address quota table 13 shown in drawing 2 B among [assigned] the server side networks, The conversion table (conversion table) 14 of the PPP circuit of each of that closed network, the address by

the side of a closed network, and the address of the assigned server side network is made. If a packet comes to the PPP line processing part 11 from a terminal and the PPP circuit will be established, with reference to the conversion table 14 applicable to the closed network and PPP circuit, to the address of the packet, address translation will be performed by the address conversion section 15, and it will be sent to the server side network. The packet from the server side network is changed into the address given by the closed network side with reference to the conversion table 14 with the address, and it gets to know which PPP circuit of which closed network it is, and it is sent out to a PPP circuit from the corresponding PPP line processing part 11.

[0057]In this R-NAT device, the processing to a packet comes to be shown in drawing 19 from a closed network. First, in advance of arrival of the first packet, it is investigated by the PPP line processing part 11 whether a PPP line connection request occurs (S1), if it is a connection request, it will attest the demand from which PPP circuit of which closed network it is (S2), and a PPP circuit will be established (S3).

[0058]If the conversion table 14 is searched by that closed network and source address (S5) and there is nothing corresponding when waiting (S4) and a packet come, the packet from the host who used that PPP circuit in this state, To the address of the packet, the address of the server side network is assigned with reference to the address quota table 13, and these relations are written in the conversion table 14 (S6). The conversion table 14 is searched with the address about an arrival packet, address translation is carried out by the address conversion section 15, and it sends to the server side network (S7). Since the PPP circuit is established, when it is in the packet waiting state of step S4 and an address is found by search of the conversion table 14, the packet which comes after that performs address translation based on (S5) and the conversion table (conversion table) 14, and sends it out to the server side network (S7). When not found, the address quota conversion table 14 is created as mentioned above.

[0059]Next, the outline functional constitution of the VNAT device (access server with a VNAT function) in drawing 8 is explained with reference to drawing 20. Two or more PPP circuit establishment parts 11 and the authentication section 12 attached to this are formed like the case of drawing 18, At the time of PPP circuit establishment, it is

recognized which PPP circuit of which closed network it is, and the VLAN tag which corresponded with the PPP circuit of the closed network on the VLAN tag table 21 as shown in drawing 9 is assigned to the PPP circuit. To the packet which came through the PPP circuit, by the packet converter 22, the VLAN tag assigned to the PPP circuit is added, and it is sent out in the server side network.

[0060]The packet which came from the server side network searches the VLAN tag table 21 with the packet converter 22 with the VLAN tag, and removes and sends out a VLAN tag to a corresponding PPP circuit. The processing to the packet from the closed network in this VNAT device comes to be shown in drawing 21. First, a PPP line connection request occurs (S1), that attestation which is the demand from which PPP circuit of which closed network is performed in advance of arrival of the first packet (S2), and a PPP circuit is established (S3).

[0061]Then, if a packet arrives at the established PPP circuit, the VLAN tag which searches the VLAN tag table 21 with (S4) and its PPP circuit of the closed network, and corresponds will be taken out (S5), this is embedded by the packet converter 22 at a packet, and it sends to the server side network (S6). When it explains with reference to drawing 12 and drawing 17 which do not use the number which distinguishes a PPP circuit as a VLAN tag, a VNAT device becomes that the VLAN tag table 21 in drawing 20 indicates correspondence with a closed network and a VLAN tag to be, As a dashed line shows in drawing 20, a PPP circuit is established, and if the VLAN tag to embed is decided, the conversion table 23 showing the relation between the VLAN tag as shown in drawing 12 or drawing 17, its PPP circuit, and the address (sauce) of the closed network of the packet will be created. The packet from the server side network determines whether to send the packet which removed the VLAN tag to which PPP circuit of which closed network by the packet converter 22 with reference to the conversion table 23 with the VLAN tag and its (destination) address.

[0062]In the processing shown in drawing 21, as a dashed line shows instead of Step S6, a VLAN tag will be embedded and sent out, and the conversion table of a VLAN tag, and the PPP circuit and address (sauce) which came will be created, and others are the same. Although this invention was applied to communication between two or more closed

networks in ****, this invention is applicable also to communication with the multiple user side network and the server side network.

[0063]

[Effect of the Invention]In this invention, each closed network is connected to the network by the side of a server by PPP connection, and various control can carry out easily at the server side by the address space assigned per closed network by attesting the closed network and the PPP circuit itself which belong at the time of this PPP connection establishment. Thereby, to the user terminal of two or more closed networks, without losing closed ****, offer of the common services customized to each closed network is physically enabled by one set of a server, and from each closed network, it can use so that a server may exist in a self-closed network respectively. The housing service which provides construction of the common server for two or more closed networks which are needed at the time of the project execution which needs the data exchange between two or more companies which will increase in number from now on and are expected to die, and operation of a procurement service, employment, etc. can be developed. By using this service, a user does not change the closed network of his company, Since the project which employment of the common server which is easily needed for a target for every project temporarily can be performed, and is undertaken by cooperating with two or more companies can be computerized smoothly, without losing closed ****, The service realized by this invention can count upon the deployment as a new supplementary service of the VPN (Virtual Private Network) service which ISP (Internet Service Provider) is offering now. It uses that the connection establishment which maintains closed **** from the server side realized by this method to the host of a closed network is possible, The server which can use the various services provided for the server side network with two or more closed networks integrative is built, and deployment of individual-oriented portal site service is also attained. Thus, this invention can count upon the use as a means to build a closed network-oriented new information distribution plat form.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The figure showing the example of composition of the system which applied the 1st invention.

[Drawing 2]The figure and B which show the example of an address mapping table [in / in A / R-NAT in drawing 1] are a figure to each closed network showing the example of quota of the address space of the server side network.

[Drawing 3]The figure showing the situation of conversion of the packet about the host 1.

[Drawing 4]The figure showing the image of network address translation.

[Drawing 5]The figure showing the utilization course of the network address space assigned to the closed network.

[Drawing 6]The figure showing the situation of the address translation in a packet.

[Drawing 7]The figure showing the relation of the feature of the 1st invention and conventional technology.

[Drawing 8]The figure showing the example of composition of the system which applied the 2nd invention.

[Drawing 9]The figure showing the example of quota of a VLAN tag.

[Drawing 10]The figure showing the operation to the packet of a VNAT function.

[Drawing 11]The figure showing the operation in the server using a VNAT tag.

[Drawing 12]The figure showing the example of matching of the VLAN tag in the 2nd invention.

[Drawing 13]The figure showing the system in the example of the 1st invention.

[Drawing 14]The figure showing the example of address assignment with the R-NAT device in drawing 12.

[Drawing 15]The figure showing the system in the example of the 2nd invention.

[Drawing 16]The figure showing the example of quota of the VLAN tag in the VNAT device in drawing 15.

[Drawing 17]The figure showing correspondence of the VLAN tag and address in modification of the 2nd invention, and a PPP circuit.

[Drawing 18]The figure showing the outline functional constitution of a R-NAT device.

[Drawing 19]The flow chart showing a part of processing in a R-NAT device.

[Drawing 20]The figure showing the outline functional constitution of a V-NAT device.

[Drawing 21]The flow chart showing a part of processing in a V-NAT device.

[Drawing 22]The figure showing the system of the conventional PPP tunneling connection.

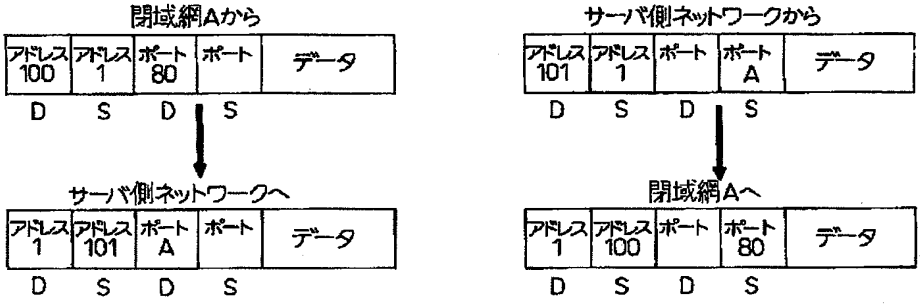
[Drawing 23]The figure showing the system of connection by the conventional NAT.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DRAWINGS

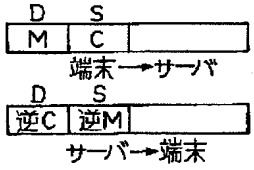
[Drawing 3]



S:ソース
D:デスティネーション

図3

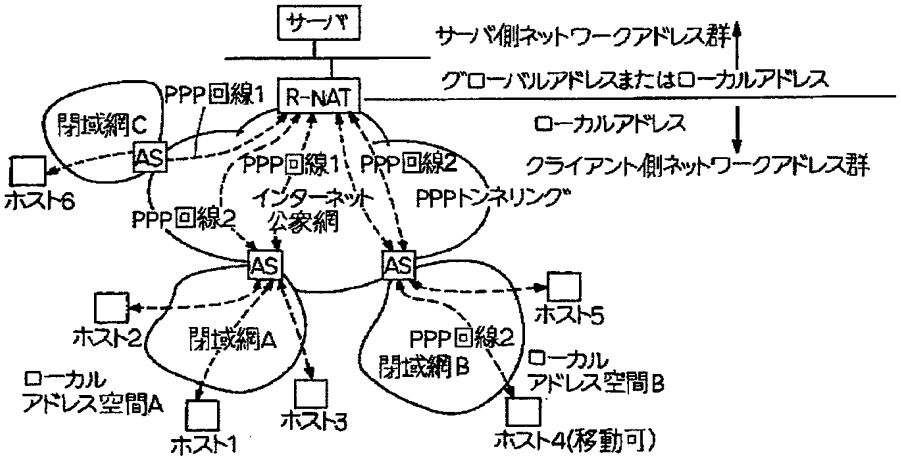
[Drawing 6]



S:ソース
D:デスティネーション
C:Compaction変換
M:Merge変換

図6

[Drawing 1]



R-NAT:Root-side NAT機能付きアクセスサーバ
AS:アクセスサーバ

図1

[Drawing 2]

A

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト1	アドレス1	—	アドレス101
ホスト2	アドレス2	—	アドレス220
ホスト3	アドレス3	—	アドレス102
ホスト4	—	アドレス11	アドレス301（静的）
ホスト5	—	アドレス22	アドレス321
Server	アドレス100	アドレス150	アドレス1

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間101-300	アドレス空間301-350
PPP回線1	アドレス空間101-200	アドレス空間311-350
PPP回線2	アドレス空間201-250	アドレス301
動的割り当て	アドレス空間251-300	—

図2

[Drawing 5]

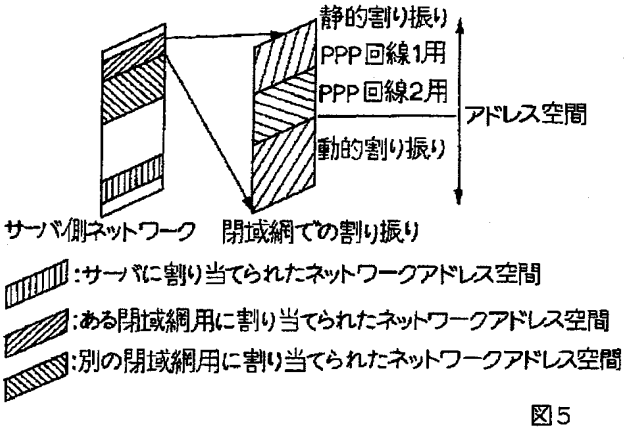


図5

[Drawing 7]

	従来のNAT	PPP トンネリング	方法1 (Root-side NAT)
ローカルアドレスの使用	○	○	○
サーバープッシュ型情報配信	×	×	○
カスタマイズドサービスの提供	△	×	○
不正アクセスパスの発生防止	×	×	○

図7

[Drawing 11]

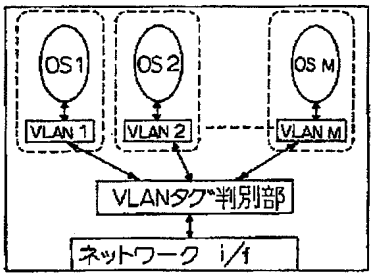


図11

[Drawing 16]

	閉域網 A	閉域網 B	閉域網 1
PPP回線1	VLAN 1-1	VLAN 2-1	VLAN 3-1
PPP回線2	VLAN 1-2	—	—

図16

[Drawing 4]

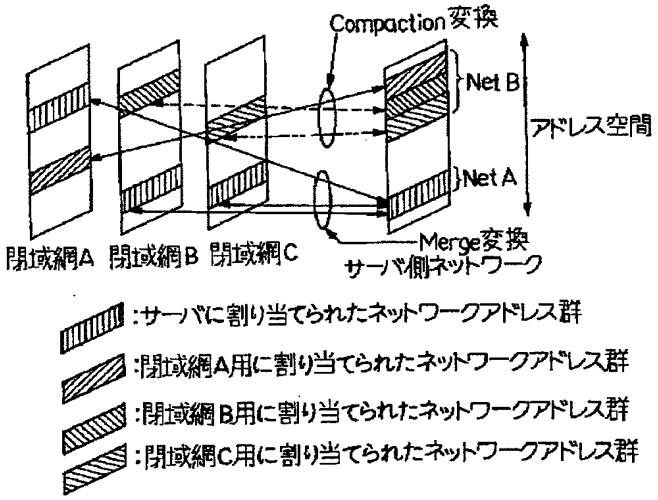


図4

[Drawing 8]

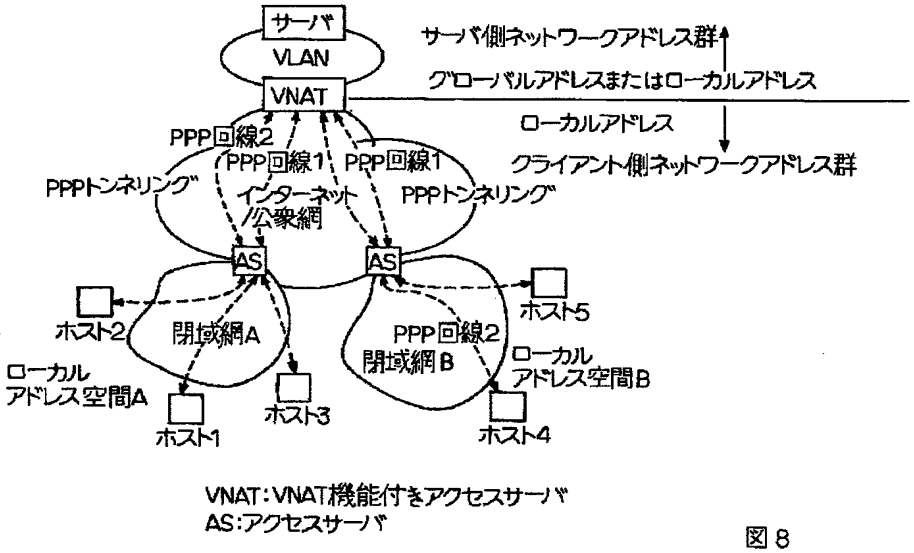


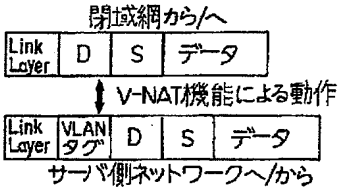
図8

[Drawing 9]

	閉域網 A	閉域網 B	VLANタグ
ホスト1	アドレス1	—	VLAN 1-1
ホスト2	アドレス2	—	VLAN 1-2
ホスト3	アドレス3	—	VLAN 1-1
ホスト4	—	アドレス11	VLAN 2-2
ホスト5	—	アドレス22	VLAN 2-1
Server	アドレス100	アドレス150	アドレス1

図9

[Drawing 10]



S:ソースネットワークアドレス
D:デスティネーションネットワークアドレス　　図10

[Drawing 12]

VLANタグ	ホストのアドレス	PPP回線番号
VLAN1	アドレス1	PPP回線1
VLAN1	アドレス2	PPP回線2
VLAN1	アドレス3	PPP回線1
VLANタグ	ホストのアドレス	PPP回線番号
VLAN2	アドレス4	PPP回線2
VLAN2	アドレス5	PPP回線1

図12

[Drawing 17]

VLAN タグ	アドレス	PPP回線番号
VLAN 1	10.0.1.13	PPP回線1
VLAN 1	10.0.3.20	PPP回線2
VLAN 2	10.0.1.30	PPP回線1
VLAN 2	10.0.1.14	PPP回線1
VLAN 3	10.1.1.1	PPP回線1

図17

[Drawing 13]

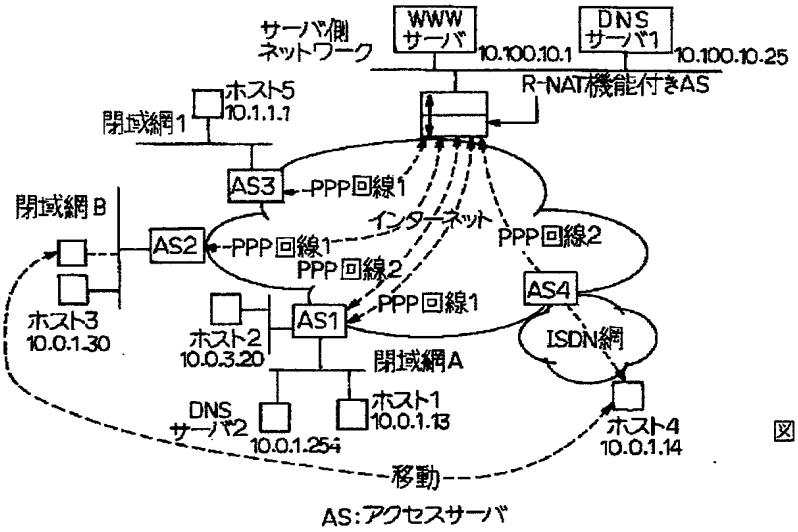


図13

[Drawing 14]

	閉域網 A	閉域網 B	閉域網 1	サーバ側ネットワーク
ホスト1	10.0.1.13	—	—	10.10.1.15
ホスト2	10.0.3.20	—	—	10.10.1.100
ホスト3	—	10.0.1.30	—	10.10.2.10
ホスト4	—	10.0.1.14	—	10.10.2.65
ホスト5	—	—	10.1.1.1	10.10.11.1
Server	10.1.1.1	10.10.15.1	10.50.1.1	10.100.10.1

図14

[Drawing 15]

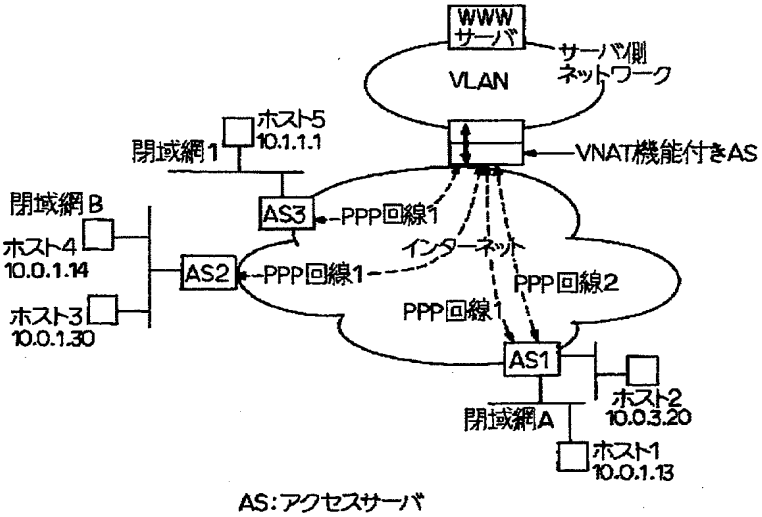


図15

[Drawing 22]

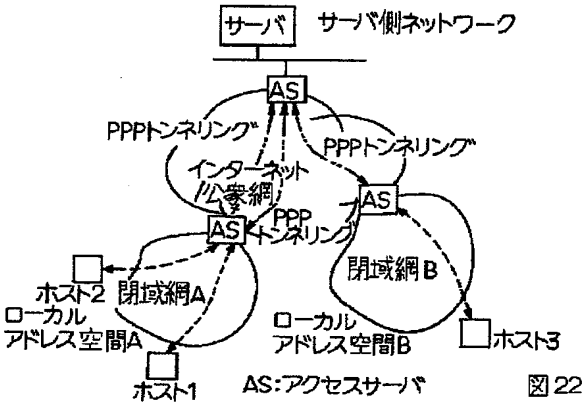


図22

[Drawing 18]

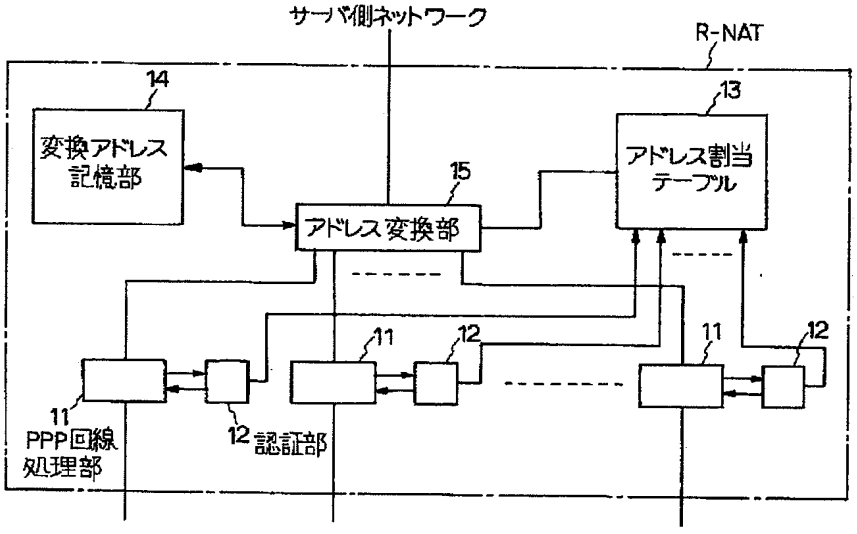


図18

[Drawing 19]

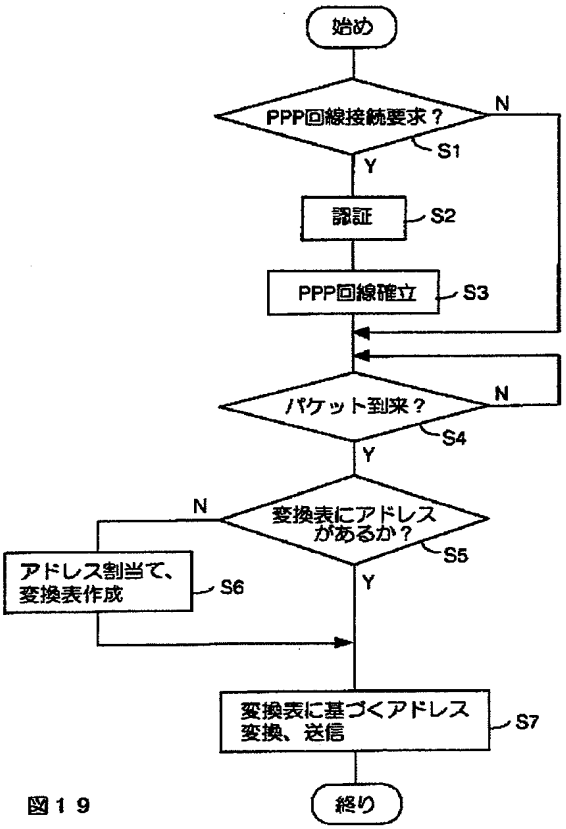


図１９

[Drawing 21]

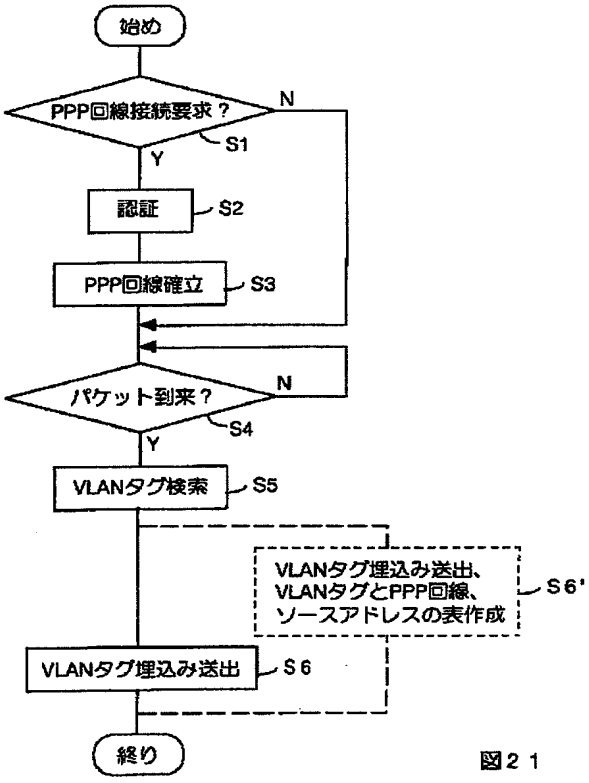


図２１

[Drawing 20]

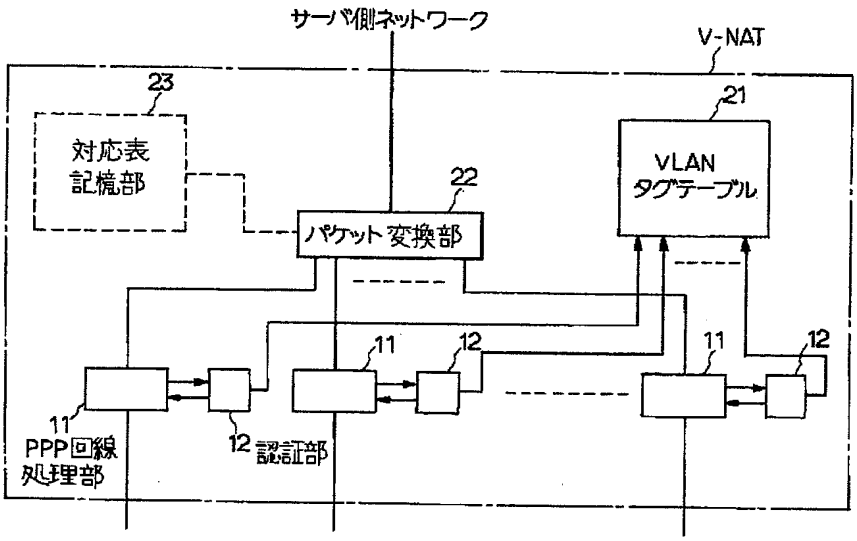


図20

[Drawing 23]

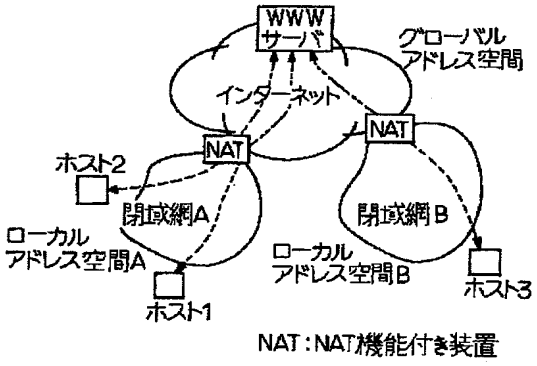


図23

[Translation done.]

Ref. 5

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－16255
（P2001－16255A）
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	
12/66				

審査請求　有　　請求項の数13　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－183067

(22)出願日　平成11年６月29日(1999.6.29)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　寺尾　和幸
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

Ｆターム(参考)　5K030 GA15 HD08 HD09 KA01 KA04
5K033 BA04 CB09 CC01 DA06 DB12

(54)【発明の名称】　ネットワーク間通信方法及びその装置

(57)【要約】
【課題】　複数閉域網とサーバ側ネットワークとの間の通信で、物理的に１台のサーバを各閉域網にそれぞれサーバがあるかのように動作させる。
【解決手段】　閉域網の端末からサーバへのＰＰＰ接続要求がアクセスサーバＡＳにあると、どの閉域網のどのＰＰＰ回線であるかを識別し、閉域網のＰＰＰ回線ごとに予め割り当てたサーバ側のアドレス空間（図２Ｂ）の中から対応する１つを選択して、その閉域網の端末のアドレスを対応付け（図２Ａ）、パケットをこのアドレス変換を行ってサーバ側ネットワークへ送る。サーバ側ネットワークからのパケットを、図２Ａを参照してアドレス変換すると共に、どの閉域網のどのＰＰＰ回線かを知り、その回線にパケットを送る。

A

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト１	アドレス１	―	アドレス 101
ホスト２	アドレス２	―	アドレス 220
ホスト３	アドレス３	―	アドレス 102
ホスト４	―	アドレス 11	アドレス 301（静的）
ホスト５	―	アドレス 22	アドレス 321
Server	アドレス100	アドレス 150	アドレス１

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間 101-300	アドレス空間 301-350
PPP回線１	アドレス空間 101-200	アドレス空間 311-350
PPP回線２	アドレス空間 201-250	アドレス 301
動的割り当て	アドレス空間 251-300	―

図２

1

【特許請求の範囲】

【請求項１】　複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol）を利用して接続して通信を行う方法において、ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
サーバ側ネットワークで、予め各ユーザ側ネットワークごとにそれぞれ割り当てた複数のアドレス空間における、上記認証したネットワーク及びＰＰＰ回線に対するアドレス空間から選んだアドレスに、そのユーザ側ネットワークのＰＰＰ回線からのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送り、
かつその変換アドレスと変換前のアドレスと、認証したユーザ側ネットワーク及びＰＰＰ回線との対応表を記憶しておき、
サーバ側ネットワークからのパケットのアドレスを上記対応表を参照して上記アドレス変換の逆変換を行って対応するユーザ側ネットワークのＰＰＰ回線へ送ることを特徴とするネットワーク間通信方法。

【請求項２】　上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのデスティネーションアドレスをサーバ側ネットワークにおける該当するアドレスに変換することを特徴とする請求項１記載のネットワーク間通信方法。

【請求項３】　上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換することを特徴とする請求項１又は２記載のネットワーク間通信方法。

【請求項４】　上記アドレスの選択はユーザ側ネットワークの利用方針に応じて動的又は静的に行うことを特徴とする請求項１乃至３の何れかに記載のネットワーク間通信方法。

【請求項５】　上記ＰＰＰ接続が確立した後にそのＰＰＰ回線からのパケットは、そのアドレスにて上記対応表を参照してアドレス変換して、サーバ側ネットワークへ送信することを特徴とする請求項１乃至４の何れかに記載のネットワーク間通信方法。

【請求項６】　複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol）を利用して接続して通信を行う方法において、ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
予め各ユーザ側ネットワークのＰＰＰ回線毎に割り当てたＶＬＡＮ（VirtualＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報を、上記認証されたユーザ側ネットワークのＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送り、
サーバ側ネットワークからのパケットのＶＬＡＮを識別する情報から求めたユーザ側ネットワークのＰＰＰ回線

2

にそのパケットを送ることを特徴とするネットワーク間通信方法。

【請求項７】　複数ユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol）を利用して接続して通信を行う方法において、ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
予め各ユーザ側ネットワークごとに割り当てたＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報を、上記認証されたユーザ側ネットワークのＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送り、
かつそのパケットのアドレスとＶＬＡＮを識別する情報とＰＰＰ回線との対応表を記憶しておき、
サーバ側ネットワークからのパケットのＶＬＡＮを識別する情報及びアドレスから上記対応表を参照してＰＰＰ回線を求めて、そのパケットをユーザ側ネットワークのそのＰＰＰ回線に送ることを特徴とするネットワーク間通信方法。

【請求項８】　複数のユーザ側ネットワークとＰＰＰ（Point-to-Point Protocol）により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、
各ユーザ側ネットワークのＰＰＰ回線ごとに割り当てられたアドレス空間を記憶するアドレス空間割り当てテーブルと、
接続してくる端末がどのユーザ側ネットワークのどのＰＰＰ回線に属するかの認証を行う手段と、
上記認証されたユーザ側ネットワークのＰＰＰ回線に対し、上記アドレス空間割り当てテーブルで割り当てられている１つのアドレスに、上記ＰＰＰ回線よりのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送るアドレス変換手段と、
上記アドレス変換されたアドレスと変換前のアドレスとの関係を記憶する変換アドレス記憶手段と、
サーバ側ネットワークからのパケットのアドレスを上記変換アドレス記憶手段を参照して変換し、かつ上記テーブルを参照して対応するユーザ側ネットワークのＰＰＰ回線へそのパケットを送るアドレス逆変換手段とを具備するアクセスサーバ装置。

【請求項９】　ユーザ側ネットワークのＰＰＰ回線からのパケットを、そのアドレスにより上記変換アドレス記憶手段を参照してアドレス変換してサーバ側ネットワークへ送る手段を備えることを特徴とする請求項８記載のアクセスサーバ装置。

【請求項１０】　上記アドレス変換手段はパケットのデスティネーションアドレスをサーバ側ネットワークの該当するアドレスに変換する手段を備えることを特徴とする請求項８又は９記載のアクセスサーバ装置。

【請求項１１】　上記アドレス変換手段は、パケット中

のサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換する手段も備えることを特徴とする請求項８乃至１０の何れかに記載のアクセスサーバ装置。

【請求項１２】　複数のユーザ側ネットワークとＰＰＰ(Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークのＰＰＰ回線とＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報との関係を記憶したＶＬＡＮ識別情報テーブルと、

ＰＰＰ接続確立時に、そのＰＰＰ回線がどのユーザ側ネットワークに属するかの認証を行う手段と、

上記認証されたユーザ側ネットワークのＰＰＰ回線と対応するＶＬＡＮを識別する情報を、上記テーブルを参照して求め、上記ＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

サーバ側ネットワークよりのパケットを、そのＶＬＡＮを識別する情報から上記テーブルを参照して対応するユーザ側ネットワークのＰＰＰ回線へ送る手段とを具備するアクセスサーバ装置。

【請求項１３】　複数のユーザ側ネットワークとＰＰＰ(Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークとＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報との関係を記憶したＶＬＡＮ識別情報テーブルと、

ＰＰＰ接続確立時に、そのＰＰＰ回線がどのユーザ側ネットワークに属するかを認証する手段と、

上記認証されたユーザ側ネットと対応するＶＬＡＮを識別する情報を上記テーブルを参照して求め、上記ＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

上記パケットのアドレスと、上記ＶＬＡＮを識別する情報と上記ＰＰＰ回線との対応表を記憶する手段と、

サーバ側ネットワークよりのパケットを、そのＶＬＡＮを識別する情報とアドレスとから、上記テーブル及び上記対応表を参照して対応するユーザ側ネットワークのＰＰＰ回線へ送る手段とを具備するアクセスサーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は異なる複数のネットワーク、特に閉域網間の通信を行うエクストラネット向けの共有サーバのホスティングサービス（各ユーザ側ネットワークに貸出すサービス）の提供や、チケット予約サービスなどパブリックなサービスをこれらのユーザ側ネットワーク（閉域網）上のサーバの持つ情報を組み込むことによりユーザ側ネットワーク（閉域網）単位でカスタマイズした（各ユーザ側ネットワークのニーズに応じた）サービスを安全に提供するなど電子商取り引きを含めた情報流通通信方法及びその装置に関する。

【０００２】

【従来の技術】今日インターネットを始めネットワークの利用は広く普及し、多くの企業においては企業内の通信費用を安く抑えかつ、安全に行うために閉域網の構築を行っている。この構築においては、専用線だけでなくＡＴＭ、ＦＲ（フレームリレー）を用いたたり、ＩＰ（インターネットプロトコル）トンネリングを利用して行っている。また、営業マンなどが外出先からこれらの閉域網に接続する場合には、ＰＰＰ（Point-to-Point Protocol)やその拡張であるＬ２ＴＰ（Layer2 tunneling Protocol)を用いている。閉域網間の通信が今後増加し、複数の閉域網で利用する共用サーバを自閉域網の閉域性を失うことなく提供したり、チケット予約サービスなどのパブリックなサービスを、各閉域網上のサーバの持つ情報と組み合わせてカスタマイズしての利用が増える。これの実現方法として、各閉域網上にサービスを提供するサーバを用意する方法があるがこれはコストがかかり、サーバを用意する側の負担が大きい。そこで、物理的には１台のサーバであるが、各閉域網からは各々別々のサーバが存在するように見え、カスタマイズしたサービスをセキュア（安全）に提供できる仮想プライベートサーバの構築を考える。

【０００３】現在、企業などの閉域網の構築においては、ネットワークの急激な普及によるＩＰアドレスの不足のために、ローカルアドレスを用いるか、インターネットなど外部に接続する時にのみ動的にグローバルアドレスを付与して外部と通信を行う方法が取られている。しかし、動的にアドレスを付与する場合、次回の接続時には同一のアドレスを付与されるとは限らないので、特に移動端末など必要時にしか接続しない／その接続自体が不安定である場合、静的にアドレスを付与することがより必要となる。また、動的にアドレスを付与する状況ではサーバ側から特定の端末への接続確立は困難であるので、ネットワーク構築時にローカルアドレスを静的に付与する場合が多い。物理的に１台のサーバでこのように構築されている閉域網に対してのサービス提供を考えた場合、（１）サーバ側ネットワークを介した不正な接続など防止、（２）接続している閉域網間におけるアドレス空間の衝突、（３）サーバから移動端末を含めた特定の端末への接続確立、という３つの問題の解決が必要となる。

【０００４】このサーバの構築には、既存技術のＬ２ＴＰ（Layer2 tunneling Protocol)に代表されるＰＰＰトンネリング技術、ＮＡＴ（Network Address Translator）に代表されるアドレス変換技術の２種類が有用な技術であるといえる。まず、ＰＰＰトンネリング技術により移動端末は時間と場所に制約されずに常に自分の閉域網への接続が可能になり、あたかもその閉域網に存在し

5

ているかのように閉域網の利用が可能になる。また、図２２に示すように閉域網Ａ，Ｂがインターネット／公衆網を介してサーバ側ネットワークと接続可とされ、各閉域網Ａ，Ｂに属するホスト（端末とも云う）にはそれぞれのローカルアドレス空間Ａ，Ｂでのアドレスが与えられており、各ホストはそれが属する閉域網の網間アクセスサーバ（ＡＳ）を通じ、ＰＰＰトンネリングを利用してサーバ側ネットワークの網間アクセスサーバと接続してサーバと接続可能とされている。この構成により、ＰＰＰ接続をサーバ側までトンネリングすることで端末に、あたかも自分の閉域網に属するサーバと接続しているように見せることができる。これにより、閉域網の持つ閉域性を維持したり、閉域網で割り当てられているローカルアドレスをそのまま使用することが可能になる。しかし、

（１）閉域網では端末にローカルアドレスを自由に割り当てるので、複数の異なる閉域網に属する端末が同一のアドレスを持つ場合が生じ、この場合は衝突が避けられない。そのため、接続先のサーバ側ネットワークから見ると同一のアドレスを持つ端末が複数存在することが発生し、この時どの端末と通信しているかを正しく認識することが出来ない。

【０００５】（２）サーバを示すアドレスを各閉域網で共通にする必要があり既存の設備への大幅な変更が必要になる場合がある。

（３）端末からの接続確立時にサーバ側からアドレスを動的に割り当てる場合、移動端末のように必要に応じてネットワークに接続してくる端末にはどのアドレスが割り当てられているか不明であって、有用なサービスであるサーバ側からの情報配信といったサービスの提供が不可能である、

（４）サーバ側のネットワークを介して、閉域側をまたぐ不正アクセス発生の可能性がある、といった問題があり、すべての課題の解決ができない。

【０００６】また、閉域網に接続しているローカルアドレスを付与されたユーザ端末がインターネット上のグローバルアドレスを付与されたサーバとの通信を行うには、ユーザ端末自身もグローバルなアドレスを持つ必要がある。しかし、前述のようにグローバルアドレスは不足するため端末にはローカルアドレスを静的に割り当てている場合が多い。この時ＮＡＴ（ネットワークアドレス変換）技術により、図２３に示すように閉域網内の通信はローカルアドレスを用いて行い、インターネット上のＷＷＷサーバとの通信には、網間境界に設けたＮＡＴを利用できる装置にあらかじめプールされたグローバルなアドレスを動的に割り当てて通信を可能にする。しかし、このＮＡＴは動的にローカルアドレスとグローバルアドレスと対応つける／アドレスとポート番号の組によりホスト（端末）間の接続の識別を行うために、（１）ホストとサーバ間の接続は動的に認識されるので、一旦

6

接続が切断した後のローカルアドレスを静的に割り当てた端末へのグローバルアドレスを持つサーバ側からの情報配信などのプッシュ型（端末からの接続確立要求なし）のサービスは不可能、（２）サーバが各閉域網ごとの認証（識別）を行うことができないため、各所属端末毎にカスタマイズしたサービスや情報を提供することが困難、（３）ＮＡＴの部分はグローバルなアドレス空間に接続しているので不正アクセスの可能性、といった問題があり、サーバ構築におけるすべての問題の解決ができない。

【０００７】また、ＮＡＴ技術自体は様々な形で拡張・利用されており、この明細書で課題としているサーバの構築に利用可能と考えられるものに、ＰＰＰと連携したＮＡＴ技術や、設定によりパケットのソースアドレスとデスティネーションアドレスの双方の変換を行えるＣｉｓｃｏ社によるＮＡＴ技術がある。ＰＰＰと連携したＮＡＴにおいては、サーバとの間にＰＰＰ接続を確立後、サーバよりふり出されたグローバルＩＰアドレスを用いて、ＰＰＰ回線を経由して外部のインターネットなどのグローバルＩＰネットワークとの通信においてＮＡＴ機能を行うものである。つまり確立されたＰＰＰ回線単位のＮＡＴが可能になっている。この技術を利用して課題のサーバの構築を考える。この技術をサーバ側の装置に導入すると、ＰＰＰ回線毎にＮＡＴを行えるので閉域網単位で利用するサービスをカスタマイズしたり、利用するサーバを各閉域網単位で変更することが容易にできる。しかし、１台のサーバによる実現を考えると、次の問題がある。

【０００８】

【発明が解決しようとする課題】（１）クライアントに相当するユーザの閉域網とサーバ側のネットワークがＰＰＰ接続により接続されるのでＰＰＰトンネリング技術を利用する場合と同様に、ローカルアドレスで構築された閉域網同士の接続においてはアドレス空間の衝突が生じることになる。特に、この技術をサーバ側に導入するとクライアントに相当する閉域網のホストから到着したパケットを受けとったサーバが、閉域網のホストを示すアドレス部分の重複によりそのパケットがどの閉域網のホストから来たのかが識別できず、正しく該当するホストへパケットを送り出すことができない。

【０００９】（２）ＰＰＰ接続確立時にふりだされたアドレスに対してＮＡＴを行うので、そのアドレスに対してサーバ側の複数のサーバの持つアドレスがマッピングされるので、ユーザの閉域網のホストから複数あるサーバのうち特定のサーバへの接続を確立することができない。確立するには、利用したいサーバの数に応じてＰＰＰ回線を確立し、ＰＰＰにより取り決められるアドレスに対してサーバのアドレスを一つ対応させることが必要になる。

【００１０】（３）サーバを示すアドレスに対して変換

を行うのだが、変換後のアドレスが閉域網のホストを示すアドレスと同一になると正しく通信が行えない。そのため、各閉域網のホストの利用するアドレスとサーバ側ネットワークのサーバのアドレスとが重ならないようにする必要があり、各閉域網でどのようなローカルアドレスを用いるかを調べて、サーバ側ネットワークのアドレスを決めるため多大な手間と時間がかかる。

【００１１】といった問題があり解決できない、Ｃｉｓｃｏ社の開発したＮＡＴ技術は、ＲＦＣ１６３１で定義されているＮＡＴとは異なり、対象となるパケットのソースアドレスとデスティネーションアドレスの双方に対してアドレスの静的／動的な割り当てによるアドレス変換表を用いてアドレス変換が可能であり、アプリケーション層との連携、特にＤＮＳ（Domain Name System）との連携によるＮＡＴに利用するアドレス変換表を作成しての柔軟な動作が可能である。このような特徴により、従来のＮＡＴ技術では難しかったグローバルアドレスを持つインターネット上のサーバなどからＮＡＴ装置の後ろに接続されているローカルアドレスで構築された閉域網上のホストへの接続確立をも可能にしている。また、受けとったパケットの外部のホストを示すアドレスがアドレス変換表にない場合はパケットを破棄したり、または、外部のネットワークに通知するアドレスを制限するなどにより閉域網の持つ閉域性を保つこともできる。この技術を用いてこの明細書で考えるサーバの構築を行うと、（１）サーバ側ネットワークもローカルアドレスで構築された閉域網の場合、アドレス空間の衝突を避け、インターネット上のサーバなど閉域網の外のホストと通信するために双方のネットワークでＮＡＴを行う。この時、閉域網間で通信を行うにはＮＡＴに利用するグローバルアドレスとホストの持つローカルアドレスを少なくとも１対１対応にしない限り接続先のホストを特定できないため通信ができずに駄目である。この場合サーバ側から閉域網のホストへの接続ができないだけでなく、複数のサーバが存在する場合には、前述の理由により特定のサーバへの接続もできない。

【００１２】といった問題がありすべてを解決できない。このように、既存の技術を用いた場合この明細書で述べているサーバ構築に生じる問題の全てを解決し得ない。

【００１３】

【課題を解決するための手段】第１発明

第１発明、第２発明においてもユーザの利用している複数のユーザ側ネットワーク（以後、ユーザ側ネットワークを閉域網として説明する）はサーバ側のネットワークにＰＰＰ（Point-to-Point Protocol）による接続を行う。このＰＰＰ接続確立時の認証において従来のユーザの認証に加え、ＰＰＰ接続を行ってきた接続元がどの閉域網のどのＰＰＰ回線かの認証を行う。第１発明によればその結果により、接続しているＰＰＰ接続がどの閉域網のどのＰＰＰ回線かを示す情報を各ＰＰＰ回線に対応付ける。そして、この情報をキーとして該当するＰＰＰ回線に割り当てられたサーバ側ネットワークのアドレスと、必要に応じて閉域網単位に決められた利用するサーバのサービスに応じたポート番号を用いて、ＰＰＰ回線を通してサーバ側ネットワークに入ってくる／から出ていくパケットに対してソースとデスティネーションの両方のネットワークアドレスと必要に応じてポート番号の変換を行う。

【００１４】この第１発明では、サーバ側ネットワークにおいて各閉域網単位にアドレス空間を独自に割り当て、その閉域網単位の方針による柔軟な利用を行う。サーバ側ネットワークにおいて各閉域網に用意されたアドレス空間は、次の方針により割り当てる。まずＰＰＰ回線単位に静的にアドレス空間を割り当てる。このアドレス空間は、サブネット単位で割り当てることにする。静的な割り当て分がなくてもよい。その場合は、全て動的にサブネット単位でＰＰＰ回線に割り当てる。そして、もし残った空間があれば割り当てられたアドレス空間を消費してしまったＰＰＰ回線に対して、ＰＰＰのＬＣＰ（設定プロトコル）などを用いて動的にＰＰＰ回線に割り当てるものとする。動的に割り当てるアドレス空間の大きさは、動的にネゴシエーションにより必要分でもよいし、一定の大きさを決めておいてもよいし、あるアルゴリズムにより徐々に大きさを大きくするなど自由に選択できる。また、動的にＰＰＰ回線を割り当てた場合、どのアドレス空間をその閉域網のどのＰＰＰ回線に割り当てたかを管理しておくことで、サーバ側から閉域網側の端末へのパケットを適切なＰＰＰ回線に送り出すことができる。

【００１５】このように閉域網単位で割り当てを含め動作が独立しているので、接続してくる閉域網のアドレス空間の衝突による問題の回避や、特定端末への接続を可能にしている。また、アドレスの変換はサーバ側で行われており、サーバ側で接続に関する制御が容易にでき、各閉域網の持つ閉域性を維持できるだけでなく、接続する閉域網側で、自閉域網のアドレス空間から自由に利用するサーバにアドレスを付与することが可能であり、導入時に伴うネットワークの設定変更は最小限に抑えることができる。以下、このアドレス変換方法を、ルートサイドＮＡＴ（以下、Root-side ＮＡＴもしくはＲＮＡＴ）と呼ぶ。

第２発明

第１発明と同様にＰＰＰ接続確立時にその回線の属するユーザの閉域網がどれかの認証を行う。そして、ＰＰＰ接続確立時の所属の閉域網の認証を終了後に、ＰＰＰ回線にそれがどの閉域網のどのＰＰＰ回線かを識別できるに十分なＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報とを対応付ける。そして、このＶＬＡＮを識別する情報をもとにスイッチング

などのＶＬＡＮ構成技術により、利用するサーバへそのＰＰＰ回線よりのパケットを運ぶ。そして、１台のサーバにおいて各ＶＬＡＮを識別する情報単位に各種処理を行うＯＳを動作させ前述のサーバを実現する。

【００１６】また、ＰＰＰ回線に閉域網を識別するに十分なＶＬＡＮを識別する情報を対応付ける場合は、パケットを受けとったＰＰＰ回線とそのパケットに示された閉域網のホストのアドレスを対応付ける。なお、この対応付けは、ＶＬＡＮを識別する情報単位に行う。これにより、ユーザのネットワークに変更を加えることなく、ＶＬＡＮを識別する情報を利用したサーバ側ネットワークの制御により容易に上述のサーバを構築、利用できる。この所属する閉域網に関する認証結果により、確立されたＰＰＰ回線に少なくとも閉域網を識別できるＶＬＡＮを識別する情報を割り当てる方法を以下、ＶＮＡＴと呼ぶ。

【００１７】

【発明の実施の形態】第１発明

まず第１発明について実施の形態を説明する。いま図１に示すシステム構成とされているとする。即ち、閉域網Ａ，Ｂ，Ｃがインターネット／公衆網とそれぞれアクセスサーバＡＳを介して接続され、インターネット／公衆網とサーバ側ネットワークが、この発明によるRoot-side ＮＡＴ機能付きアクセスサーバＲ－ＮＡＴを介して接続されている。閉域網Ａ，Ｂにおいて各ホスト（端末）に対して図２Ａに示すようにアドレスが割り当てられている。つまり閉域網Ａの持つアドレス空間において、ホスト１にはアドレス１、ホスト２にはアドレス２、ホスト３にはアドレス３、利用するServerにはアドレス１００が割り当てられているとする。Serverはサーバ側のネットワークにおかれているホストの一つであり、このServerはサーバ側のネットワークにおいて、アドレス１が与えられている。さらに、サーバ側のネットワークにおいては図２Ｂに示すように閉域網Ａ，Ｂに対してそれぞれ固有のアドレス空間が用意されている。閉域網Ａから接続してくる端末用にアドレス群１０１～３００を用意しており、そのうち、ホスト１とホスト３の利用しているＰＰＰ回線１から接続してくる端末用にアドレス群１０１～２００を、ホスト２が利用しているＰＰＰ回線２から接続してくる端末用にアドレス群２０１～２５０をそれぞれ割り当てている。そして、残りのアドレス群２５１～３００は、前述の割り当てを使い切った場合に、ＰＰＰ回線１，２に対して動的に必要に応じて割り当てる。閉域網Ｂの持つアドレス空間において、ホスト４にはアドレス１１、ホスト５にはアドレス２２、利用するServerにはアドレス１５０が各々割り当てられている。さらに、サーバ側のネットワークにおいては閉域網Ｂから接続してくる端末用にアドレス群３０１～３５０を用意しており、そのうち、アドレス群３０１～３１０までは閉域網Ｂの端末が直接確立するＰＰＰ回線に静的に割り当てられている。また、３１１～３５０まではＰＰＰ回線１に割り当てられており、このＰＰＰ回線を利用してくるホストにサーバ接続時に動的に割り当てるものとする。このように、サーバ側のネットワークで各閉域網単位にアドレス空間をプールし、アドレス空間を閉域網の利用方針に応じてＰＰＰ回線に割り当て、そこから更に該当するＰＰＰ回線を利用するホストへ静的、動的を含め柔軟に割り振る。

【００１８】また、各閉域網におかれたアクセスサーバＡＳとRoot-side ＮＡＴの機能を持つ装置Ｒ－ＮＡＴとの間はＰＰＰ接続されている。また、閉域網の端末は、このＰＰＰ接続を利用してサーバを利用するか、ＰＰＰトンネリングを利用して直接サーバ側におかれたRoot-side ＮＡＴ機能付き装置（Ｒ－ＮＡＴ）とＰＰＰ接続を行いサーバを利用する。

【００１９】そこで、サーバ側のネットワーク上の物理的に１台のサーバを各閉域網にあたかも各々存在するように仮想的に見せ、各閉域網の閉域性を失うことなく複数閉域網において利用可能にするのが、このRoot-side ＮＡＴである。このRoot-side ＮＡＴはサーバ側で各閉域網毎に、あらかじめ用意したアドレスを割り当てるに際し、閉域網とのＰＰＰ接続確立時に接続を要求している端末が正しいかどうかというホストに関する従来の認証だけでなく、接続してくる端末がどの閉域網のどのＰＰＰ回線に属するかの認証を行う。この結果を基に、あらかじめその閉域網のＰＰＰ回線に用意されたアドレス群の中から端末に静的にアドレスが割り振られている場合は該当するものを、そうでない場合は、ＰＰＰ回線単位に用意されたアドレス空間から端末に動的にアドレスを割り振る。

【００２０】図１において、ホスト１が接続してきた時、ＰＰＰ回線がまだ確立していない場合、利用しているＡＳ（アクセスサーバ）からＰＰＰ回線の確立がはじまり、この時、このＰＰＰ回線が閉域網ＡからのＰＰＰ回線１であることの認証を行う。そして、この閉域網ＡのＰＰＰ回線１用にプールされたアドレス空間からアドレスをホストに対して動的に割り当てる。今回の場合、ＰＰＰ回線１には、図２Ｂに示すようにアドレス空間１０１－２００が与えられており、この空間から動的に与えるので、ホスト１には、利用されていないアドレス１０１をサーバ側ネットワークにおいて割り当てる。つまり、ＲＮＡＴにより閉域網ＡのＰＰＰ回線１よりのパケットについて閉域網Ａで与えられているアドレス１がアドレス１０１に変換されることになる。この関係が図２Ａに示すように表として記憶される。その後、閉域網ＡのＰＰＰ回線１を通してホスト１からパケットが到来すると、そのアドレス１により図２Ａの表を参照してサーバ側ネットワークのアドレス１０１に変換される。同様に、ホスト３からのパケットが来た場合は、ＰＰＰ回線１からということで同一のアドレス空間から動的にホス

ト３に、利用されていないアドレス１０２が割り当てられ、ＲＮＡＴによりホスト３の持つアドレス３がアドレス１０２に変換される。ホスト２がサーバに接続する場合、別のＰＰＰ回線であるＰＰＰ回線２を利用しているので、ＰＰＰ回線２用に用意されたアドレス空間２０１－２５０から割り当てることになり、利用されていないアドレス２２０がサーバ側のネットワークで割り当てられ、ＲＮＡＴによりアドレス２がアドレス２２０に変換される。

【００２１】ホスト４は、ＰＰＰトンネリングを利用してサーバ側の装置に直接ＰＰＰ接続してきており、ＰＰＰ回線の確立がはじまり、この時、同様の認証によりこのＰＰＰ回線が閉域網ＢからのＰＰＰ回線２であることが認証される。そして、この閉域網ＢのＰＰＰ回線２には静的にアドレス３０１が割り当てられているので、ＲＮＡＴによりホスト４の持つアドレス１１がアドレス３０１にサーバ側ネットワークにおいて変換されることになる。ホスト５がサーバに接続する場合、利用するＰＰＰ回線が閉域網ＢのＰＰＰ回線１であることが認証され、ＰＰＰ回線１に用意されたアドレス空間３１１－３５０から利用されていないアドレスが動的にホスト５に割り当てられる。今回は、アドレス３１１が割り当てられている。ホスト５からサーバへのパケットは、ＲＮＡＴによりホスト５の持つアドレス２２に対してアドレス３１１へと変換される。

【００２２】また、接続先に指定されたServerのアドレスもサーバ側のネットワークにおいてServerに割り当てたアドレスへの変換を行う。今回、閉域網Ａに関してはServerのアドレス１００がアドレス１に、閉域網Ｂに関してはServerのアドレス１５０がアドレス１に変換されることになる。閉域網単位に割り当てたアドレスを基にした利用するサービスの制限も可能であるが、閉域網単位に利用するサーバのポート番号を決めておくことで、サーバのポート番号により、物理的に１台のサーバにより閉域網単位のサービス提供を可能にする。今回、Serverにおいて閉域網Ａ向けのサービスは、ポート番号Ａで、閉域網Ｂ向けのサービスは、ポート番号Ｂで提供されているとする。

【００２３】Root-side ＮＡＴは、このアドレスの対応付けとポート番号を基にパケットのソースとデスティネーション両方のネットワークアドレスとポート番号の変換とをサーバ側の管理のもとで行う。実際、ホスト１がServerのWWW Server （ポート番号８０）を利用する場合、ホスト１のパケットはＲＮＡＴにより図３に示すような変換動作が行われることになる。図３Ａはホスト１からサーバへのパケット、図３Ｂはサーバからホスト１へのパケットの各Ｒ－ＮＡＴでの変換を示す。

【００２４】つまり、Root-side ＮＡＴにおけるアドレス変換部分をまとめると、図４に示すようになる。この図においてＮｅｔＡは、サーバ側のネットワークのアドレス空間においてServerが存在しているネットワークのアドレス群、ＮｅｔＢはサーバ側のネットワークのアドレス空間における各閉域網用に用意されたアドレス群をまとめたものである。また、図５に示すように各閉域網用に用意されたアドレス群は、端末あるいは、ネットワークに接続している各ＰＰＰ回線に静的に割り当てられ、残りの空間は、静的に割り当てられている空間が足らなくなった場合に、不足しているＰＰＰ回線に対して要求に応じて動的に割り当てるために用いる。動的に割り当てられた空間は、割り当て時にどのＰＰＰ回線に割り当てたかを管理することで、パケットを適切なＰＰＰ回線に送出することができる。このように、サーバ側ネットワークに用意された空間は、各空間の利用者である閉域網が利用の方針を選択できる。各閉域網における端末のアドレスをサーバ側において閉域網毎にあらかじめ用意されたアドレスに各々対応付けることをコンパクション（Compaction）変換、各閉域網において割り振られたServerのアドレスをサーバ側のネットワークにおけるサーバのアドレスに変換することをマージ（Merge)変換と呼ぶことにする。また、逆Compaction変換は端末に割り振られたアドレスからどの閉域網のどのＰＰＰ回線かを図２Ａ，Ｂを参照して識別し、その閉域網における端末のアドレスに変換する。逆Merge 変換は逆Compaction変換から得られるどの閉域網に属する端末かの情報から、サーバのアドレスを閉域網におけるサーバのアドレスに図２Ａを参照して変換する。そして、どの閉域網のどのＰＰＰ回線かの識別により適切な閉域網の適切なＰＰＰ回線へとパケットを送り出す。この時、端末からサーバへのパケット、サーバから端末へのパケットのソースとデスティネーションアドレスに上記の変換を図６に示すように行う。また、利用しているサーバのポート番号にも関してサーバ側ネットワークにおいて閉域網単位に決めたポート番号から、閉域網において利用されているポート番号へと変換する。

【００２５】この各閉域網毎に与えられたアドレス空間は、所属する閉域網に関する認証の結果割り当てることから、各アドレスがどの閉域網であるかは認証されているので、この異なる閉域網のアドレス間の接続をサーバ側で禁止することで、結果として閉域網間の通信を禁止し、閉域網の持つ閉域性を確保できることになる。さらに、各閉域網に割り当てられたこのアドレス空間を基にしたり、各閉域網に対してサーバにおいて利用できるポート番号を決めることで提供するサービスを閉域網毎にカスタマイズすることが可能になる。従来技術と第１発明（ルートサイドＮＡＴ）の特徴を図７にまとめて示す。

第２発明

第２発明が適用されるシステム構成を図８に示す。閉域網Ａ，Ｂがそれぞれアクセスサーバ５を介してインターネット／公衆網と接続され、またサーバ側ネットワー

クがＶＮＡＴ機能付きアクセスサーバＶＮＡＴを介してインターネット／公衆網と接続されている。ＶＮＡＴ機能付きアクセスサーバＶＮＡＴでは図９に示すようにＶＬＡＮタグを各閉域網の各ＰＰＰ回線に割り当てる。以下、この割り当てによる変更をＶＮＡＴと呼ぶ。各閉域網におかれたアクセスサーバＡＳは、サーバ側ネットワークにあるＶＮＡＴ機能を持つアクセスサーバＶＮＡＴにＰＰＰ接続を行う。

【００２６】ホスト１，２，３は、いずれも閉域網Ａのホストであることから、閉域網Ａを示すＶＬＡＮを利用する時に利用するＶＬＡＮを識別する情報、例えばＶＬＡＮタグとしてＶＬＡＮ１－ｘが割り当てられる。次に、同一閉域網からの複数のＰＰＰ回線を識別するために子番号ｘを割り当てる。ホスト１と３は、同一のＰＰＰ回線１から来ており、ＶＬＡＮタグとしてＶＬＡＮ１－１がＰＰＰ回線１と対応付けされている。また、ホスト２は、閉域網ＡのＰＰＰ回線２を利用して接続していることから、ＶＬＡＮタグとしてＶＬＡＮ１－２が該当するＰＰＰ回線２に対応付けされている。同様に、ホスト４，５は閉域網Ｂに属するホストであることから、閉域網Ｂを示すＶＬＡＮタグとしてＶＬＡＮ２－ｘが割り当てられることになる。閉域網Ａの場合と同様にＰＰＰ回線を識別するために、ホスト４にはＶＬＡＮ２－２がホスト５にはＶＬＡＮ２－１が割り当てられる。

【００２７】図１０に示すようにＶＮＡＴ機能を持つ装置ＶＮＡＴにおいてＶＬＡＮタグの割り当てに基づき閉域網から受け取ったパケットにこのＶＬＡＮタグを埋め込む。そして、このパケットは、ＩＥＥＥ８０２．１０やＶＬＡＮ対応のスイッチング機能などの既存のＶＬＡＮ技術によりServerまでこのＶＬＡＮタグに基づき運ばれる。パケットを受け取るServerは、図１１に示すようにＶＬＡＮタグ毎に別々の処理を行うために複数のＯＳが動作できるように変更し、閉域網を識別できる単位のＶＬＡＮタグに対し１つのＯＳが動作するようにする。つまり、ＶＬＡＮ１－ｘのタグに関する処理を行うためのＯＳ１，ＶＬＡＮ２－ｘのタグに関する処理を行うためのＯＳ２をという具合に１台のマシンの中で複数のＯＳを動作させることになる。サーバ側のネットワークにおいては、ＶＬＡＮタグを基にパケットの配送が行われるのでサーバ側のネットワーク上のサーバを含めて仮想的な閉域網を構築することができるので、パケットのアドレスに関してサーバ側では何ら変換を行う必要はない。このように、１台のサーバにおいてＶＬＡＮタグ毎にＯＳを動作させることでサーバ側の管理の下、閉域網の持つ閉域性を失うことなく仮想プライベートサーバを構築できる。

第２発明の変形

第２発明の変形例を以下に示す。ホスト１，２，３はいずれも閉域網Ａのホストであることから、閉域網Ａを示すＶＬＡＮタグとしてＶＬＡＮ１が割り当てられる。次

に、同一閉域網からの複数のＰＰＰ回線が確立された場合に、パケットを受けとったＰＰＰ回線へとそのホスト宛のパケットを送り返すことができるように、ホストを示すアドレスとＰＰＰ回線を対応付ける。ホスト１と３は、同一のＰＰＰ回線１から来ており、各々のアドレスがＰＰＰ回線１へ対応付けられる。また、ホスト２は、閉域網ＡのＰＰＰ回線２を利用して接続していることから、ＶＬＡＮタグとしてはＶＬＡＮ１が割り当てられるが、ホスト２のアドレス２がＰＰＰ回線２に対応付けされる。

【００２８】同様に、ホスト４，５は閉域網Ｂに属するホストであることから、閉域網Ｂを示すＶＬＡＮタグとしてＶＬＡＮ２が割り当てられることになる。閉域網Ａの場合と同様に受けとったＰＰＰ回線にパケットを送り返すためにホストのアドレスとＰＰＰ回線とを対応付ける。この場合、ホスト４のアドレスがＰＰＰ回線２へ、ホスト５のアドレスがＰＰＰ回線１に対応付けられる。図１２に示すようにこのＰＰＰ回線とホストのアドレスの対応付けはＶＬＡＮタグ単位に行うので、ＶＬＡＮ１，ＶＬＡＮ２の各々独立して対応付けが行われる。参考までに、ＶＬＡＮ１に関する対応付けは以下のようなものとなる。この対応付けにおいて最新の接続時刻も合わせて管理して、タイムアウトを設けるなどによりセキュリティを高めることも出来る。サーバからのパケットを受けとるとこのＶＮＡＴ変換を行っている装置において、パケットに埋め込まれているＶＬＡＮタグをキーとして、まず検索する対応表を決め、次にパケットに埋め込まれているデスティネーションアドレス（ホストのアドレス）をキーとして対応表を検索し、送り出すべきＰＰＰ回線を調べる。その結果により、パケットを受けとったＰＰＰ回線へと送出することができる。

具体例

この発明の方法により可能となる仮想プライベートサーバを利用した具体例として、複数業者を対象とする調達業務の例を用いて述べる。今回、企業１が調達のために各々企業Ａ，Ｂに調達依頼をし、どちらか良い方を選択するために企業間でデータの登録、交換しあうことが必要となる場合での具体例である。

第１発明の具体例

図１３に示すようなネットワーク構成になっているとする。閉域網Ａ，Ｂ，１はそれぞれアクセスサーバＡＳ１，ＡＳ２，ＡＳ３によりインターネットと接続され、ＩＳＤＮ網がアクセスサーバＡＳ４によりインターネットと接続され、サーバ側ネットワークがルートサイドＮＡＴ機能付きアクセスサーバＲ－ＮＡＴによりインターネットと接続されている。また、ルートサイドＮＡＴ機能を持つ装置Ｒ－ＮＡＴにおいては図１４に示すようにアドレスの変換表を作成して動作する。変換表の作り方は後述する。ここで、閉域網Ｎは、企業Ｎの持つ閉域網を意味するものとする。サーバ網のネットワークにおか

れたルートサイドＮＡＴ機能付き装置Ｒ－ＮＡＴと各閉域網に置かれたアクセスサーバＡＳ１，ＡＳ２，ＡＳ３との間はトンネリングを利用してＰＰＰ接続される。また、ＩＳＤＮなどを利用してアクセスサーバＡＳ４に接続し、これを経由して閉域網に属するホストが直接サーバ側ネットワークにある装置Ｒ－ＮＡＴとＰＰＰ接続を行うこともできる。

【００２９】各閉域網のホストには所属する閉域網の持つアドレス空間から図１２に示すようにアドレスが各々割り振られている。このRoot-side ＮＡＴの機能を利用するために、サーバ側のネットワークにおいて各閉域網のためにアドレス空間をプールしてある。この例において、閉域網Ａにはエアアドレスで表わして１０．１０．１．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網Ａから接続してくる端末にアドレスを割り当てる。同様に、閉域網Ｂには１０．１０．２．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網Ｂから接続してくる端末に、閉域網１には１０．１０．１１．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網１から接続してくる端末にアドレスを割り当てる。

【００３０】閉域網Ａにおいて、ホスト１は１０．０．１．１３、ホスト２は１０．０．３．２０、利用するWWW Server に１０．１．１．１が割り当てられているとする。実際には、WWW Server はサーバー側のネットワークにおかれていて、このWWW Server はサーバー側のネットワークにおいて、１０．１００．１０．１が割り当てられ、異なる複数の閉域網に属する端末に対してサービスを提供している。サーバ側のネットワークにおいて閉域網Ａに割り当てられているアドレス空間１０．１０．１．０サブネットマスク２５５．２５５．２５５．０のうち、１０．１０．１．０サブネットマスク２５５．２５５．２５５．１９２はＰＰＰ回線１に、１０．１０．１．６４サブネットマスク２５５．２５５．２５５．１９２は、ＰＰＰ回線２に割り当てられている。そして、残りの空間１０．１０．１．１２８サブネットマスク２５５．２５５．２５５．１２８は動的にＰＰＰ回線１，２からの要求に応じてサブネットワーク単位で要求してきたＰＰＰ回線に割り当てるためにとってある。また、閉域網Ａの端末がWWW Server を利用する場合、サーバ側のネットワークにおいて、ポート番号８０８０番で閉域網Ａ用のサービスを展開するように設定されている。

【００３１】今、ホスト１がWWW Server を利用する場合、アクセスサーバ１（以下、ＡＳ１）から確立されるＰＰＰ回線１を利用するようになっている。もし、ＡＳ１とサーバ側のRoot-side ＮＡＴ機能付きＡＳ（以下、ＲＮＡＴ装置）との間にＰＰＰ回線１が確立していない場合、まずＰＰＰ接続を確立する。この時、ホストの認証だけでなくどの閉域網のどのＰＰＰ回線かを認証する。この場合、閉域網ＡのＰＰＰ回線１であることが認証される。次に、閉域網ＡのＰＰＰ回線１用にサーバ側ネットワークにおいて割り当てられているアドレス空間に利用していないアドレスがあるかをチェックする。今回の場合使用されていないアドレスがあるとし、その空間からホスト１に動的に１０．１０．１．１５が割り当てられる。もし、すでにＰＰＰ回線１用の空間がすべて使用されている場合、ＡＳ１がＰＰＰのＬＣＰなどを利用して必要な分のアドレス空間を要求し、これに応じてＲＮＡＴ装置において、閉域網Ａの持つ動的に割り当てるために用意されている空間１０．１０．１．１２８サブネットマスク２５５．２５５．２５５．１２８から要求のうち許可分を新たに複数のＰＰＰ回線１に割り当て、その中から動的にホスト１にアドレスを割り当てることになる。この時、割り当てる空間がどのＰＰＰ回線に割り当てたかをＲＮＡＴ装置で管理し、これによりパケットを適切なＰＰＰ回線へと送り出せる。動的に割り当てるのは、サブネット単位の要求分を割り当てる他に、決まった一定のサブネット空間分でもよいし、徐々にサブネット空間を単位として大きくしていってもよい。

【００３２】ホスト２は、閉域網Ａにおいてアドレスが１０．０．３．２０であり、ＡＳＩとＲＮＡＴ装置間に確立されるＰＰＰ回線２を利用してサーバに接続する。ホスト１が接続する場合と同様に、このＰＰＰ接続確立時にこのＰＰＰ回線が閉域網Ａに属するＰＰＰ回線２であることが認証される。そして、閉域網ＡのＰＰＰ回線２用に用意された空間１０．１０．１．６４サブネットマスク２５５．２５５．２５５．１９２から使用されていないアドレスを検索し、ホスト２に割り当てる。今回、ホスト２には、１０．１０．１．１００が動的に割り当てられる。もし、あらかじめ用意された空間がすべて使用されていたら、ホスト１の時と同様にして動的にアドレス空間をＰＰＰ回線２に割り当て、その空間から動的にホスト２に割り当てる。このようにして、接続してきたホストにサーバ側のネットワークにおいてアドレスが割り当てられ、ＲＮＡＴ機能に必要なアドレス変換表が作られる。

【００３３】ホスト１からWWW Server への場合、ＲＮＡＴ装置においてパケットのソースアドレスを１０．０．１．１３から１０．１０．１．１５へ、デスティネーションアドレスを１０．１．１．１から１０．１００．１０．１へと変換する。また、WWW Server を利用するために、サーバのポート番号８０にホスト１は利用要求を出すが、ＲＮＡＴ装置において閉域網Ａ用のサービスを提供しているサーバのポート番号８０８０にポート番号も変更して、変換後サーバ側ネットワークのルーティングにより正しくサーバに送られ、閉域網Ａ向けのサービスの利用が行われる。

17

【００３４】逆にWWW Server からホスト１へのパケットは、デスティネーションアドレスを１０．１０．１．１５から閉域網Ａに属するホスト１であることとＡＳ１から確立されているＰＰＰ回線１向けのパケットであることを識別し、アドレスを１０．０．１．１３へと変換する。次にホスト１が閉域網Ａに属しているという情報からソースアドレスを１０．１００．１０．１から１０．１．１．１へ変換する。そして、ポート番号も８０８０からホストが送ってきたパケットに指定されていたポート番号８０へと変換される。この変換後、受け取ったパケットの持つデスティネーションアドレスに基づく情報により適切なＰＰＰ回線である閉域網ＡのＰＰＰ回線１へパケットを送り出す。

【００３５】同様に、閉域網Ｂの場合について述べる。閉域網Ｂにおいて、ホスト３は１０．０．１．３０、ホスト４は１０．０．１．１４、利用するWWW Server に１０．１０．１５．１を割り当てているとする。実際には、WWW Server はサーバ側のネットワークにおかれていて、このWWW Server は前述同様、サーバ側のネットワークにおいて、１０．１００．１０．１が割り当てられている。サーバ側のネットワークにおいて、閉域網Ｂに割り当てられているアドレス空間は、１０．１０．２．０サブネットマスク２５５．２５５．２５５．０であり、閉域網Ｂでは、端末自身がＲＮＡＴ装置に直接ＰＰＰ接続する利用も行われており、そのために、１０．１０．２．６４．サブネットマスク２５５．２５５．２５５．１９２の空間をそれらのために用意し、各ＰＰＰ回線と１対１対応にアドレスを静的に割り振っている。今回、ＰＰＰ回線２以降が端末から直接確立されるＰＰＰ回線とし、ＰＰＰ回線２には、１０．１０．２．６５が割り当てられており、他の該当するＰＰＰ回線もアドレスが１つ静的に割り当てられている。また、ＡＳ２から確立されるＰＰＰ回線１用には１０．１０．２．０サブネットマスク２５５．２５５．２５５．１９２の空間を静的に割り当てており、このＰＰＰ回線を利用するホストにアドレスはこの空間から動的に割り当てられる。残りの空間１０．１０．２．１２８サブネットマスク２５５．２５５．２５５．１２８は割り当て分を使用したＰＰＰ回線１からの要求に応じて動的に割り当てるために用意してある。

【００３６】ホスト３はＡＳ２により確立されているＰＰＰ回線１を利用して接続しているので、閉域網Ａのホスト１や２の場合と同様に、利用しているＰＰＰ回線が閉域網ＢのＰＰＰ回線１であることが認証されると、静的に割り当てられた空間１０．１０．２．０サブネットマスク２５５．２５５．２５５．１９２に使用されていないアドレスがあるかを検索し、あればその中から任意なものを割り振る。今回、ホスト３にはサーバ側ネットワークにおいて、１０．１０．２．１０が割り当てられる。ホスト４は、今、移動しており最寄りのＡＳ４に着

18

呼し、ＰＰＰトンネリングを利用してＲＮＡＴ装置に対して直接ＰＰＰ回線を確立する。この確立時に、ＰＰＰ回線が閉域網ＢのＰＰＰ回線２であることが認証され、ＰＰＰ回線２は静的にアドレスが１つ割り当てられており、この例では割り当てられているアドレス１０．１０．２．６５がホスト４のアドレスとなる。また、WWW Server のアドレスは閉域網Ａの場合と同じである。また、利用するサービスを示すポート番号は、閉域網Ｂにはポート番号８０８１が割り当てられている。

【００３７】実際のホストからWWW Server （ポート番号８０）への通信時には、ホスト１，２の場合と同様に図１４に示す変換表などによりＲＮＡＴ装置において、パケットの持つソースとデスティネーションアドレスを各々変換し、さらにポート番号に関して、８０から閉域網Ｂに対して指定されている８０８１番に変換される。逆にWWW Server からホストへのパケットも、前述と同様にパケットの持つソースとデスティネーション双方のアドレスとポート番号を変換する。この変換時に、パケットのデスティネーションアドレスによりホストの所属する閉域網がどれであるか、その閉域網から複数のＰＰＰ回線が存在する場合には、どのＰＰＰ回線へ送り出すかを判断できる。また、この情報を基にサーバに対して接続しているポート番号も変換される。そして、アドレスとポート番号が変換後、適切なＰＰＰ回線へと送出される。例えば、ホスト３へのパケットの場合は、１０．１０．２．１０がデスティネーションアドレスとして与えられているので、これにより閉域網ＢのＰＰＰ回線１へ送り出せば良いパケットであることが識別されて送り出される。

【００３８】閉域網１のホスト５の場合も同様に動作し、閉域網１の決めたアドレス空間の割り当て方針によりアドレスがホスト５に割り当てられ、図１３に示すような表が作られ、これを利用してアドレス変換がホスト５に関して行われる。また、閉域網１用に決められたサーバ利用時のポート番号８０８８とすると、ポート番号に関しても変換が行われる。サーバ側ネットワークからホストへのパケットに対しても前述と同様の仕組みにより適切な閉域網の適切なＰＰＰ回線へと送られる。

【００３９】ここで、アドレスは所属する閉域網を認証した結果としてサーバ側のネットワークにおいて割り振られるので閉域網を示すという意味においてアドレスは保証されていることになり、このアドレスを基に制限を行うことは、閉域網単位での制限を行うことと同等である。つまり、アドレス１０．１００．１０．１を持つWWW Server は、１０．１０．１．０サブネットマスク２５５．２５５．２５５．０、１０．１０．２．０サブネットマスク２５５．２５５．２５５．０、１０．１０．１１．０サブネットマスク２５５．２５５．２５５．０の各アドレス空間からの接続のみを許可することで、これ以外のアドレス、つまり他の閉域網からの利用

を容易に制限ができる。これにより、限られた閉域網間での通信を閉域性を保ちながらできる。また、アドレスを利用したデータへのアクセス制限だけでなく、今回のように閉域網単位で利用するポート番号を決めておき、そのポート番号単位にそれに応答するプログラムを動作させ、参照できるデータ、参照して変更できるデータなどを設定しておくことで物理的に一台のサーバによる複数閉域網向けにカスタマイズしたサービスが実現できる。

【００４０】今回の場合、閉域網Ａ，Ｂに割り当てているポート番号８０８０と８０８１に対して動作しているプログラムがアクセス、操作できるデータを各々区別することで、同一サーバ上にデータがあっても閉域網Ａは自分の登録したデータは参照・変更はできるが、閉域網Ｂの登録したデータは変更する事はもちろん見ることもできないようにできる。逆に、閉域網１に割り当てたポート番号８０８８に対して動作しているプログラムは、先のポート番号８０８０と８０８１で動作しているプログラムがそれぞれアクセス、操作できるデータの両方にアクセスすることが出来るようにすれば、閉域網１のホストは、閉域網Ａ，Ｂ双方が独立して管理するデータを参照できる。これにより、今回の例としている調達業務において要求される注文主の企業１が注文先である企業Ａ，Ｂ双方のデータを自由に見ることができるという課題がクリアされる。これは、今回のようにポート番号で制限を行ってもよいし、閉域網単位に割り当てたアドレス空間を用いて制限を行っても良い。また、異なるアドレス空間における通信を禁止することで、サーバ側のネットワークを介した異なる閉域網間での通信を防止でき、閉域網の持つ閉域性を維持することができる。さらには、接続先のサーバのアドレスもサーバ側で管理できるので、複数のサーバを用意しておけばサーバの負荷に応じてアドレスの変換を行うことでサーバの負荷分散も可能になる。

【００４１】次に、ＩＰネットワークによる通信時に重要な働きをするＤＮＳ（Domain Name System）サーバとの動きを、閉域網Ａとサーバ側ネットワークとの通信時を例として述べる。図１２において、まずユーザの閉域網に属するホストがサーバ側のネットワークのホストに接続する場合を述べる。閉域網Ａに属するホスト１がサーバ側ネットワークのＷＷＷサーバに接続するために、閉域網Ａ上のＤＮＳサーバ２に接続したいＷＷＷサーバのアドレスを問い合わせる。閉域網Ａのアドレス空間においてＷＷＷサーバに対してアドレスが割り当てられているので、ＤＮＳサーバ２は閉域網Ａで該当するサーバに割り当てられたアドレス１０．１．１．１をホスト１に返す。そして、ホスト１は、ソースアドレスを自分の持つアドレス１０．０．１．１３、デスティネーションアドレスをサーバの持つアドレス１０．１．１．１、デスティネーションのポート番号８０としたパケットを送出する。そして、閉域網Ａのネットワークにおいて１０．１．１．１宛のパケットをＡＳ１へ届くように正しくルーティングを設定しておくことで、このパケットは、ＡＳ１に届き、必要ならばＰＰＰ回線を確立してサーバ側ネットワークのＲＮＡＴ機能付き装置まで運ばれる。このパケットを受け取ったＲＮＡＴ機能付き装置はパケットのデスティネーションアドレスを自身の持つ変換表を基に、１０．１．１．１から１０．１００．１０．１へと変換する。次に、ソースアドレスの１０．０．１．１３を変換表の中において検索する。検索した結果、該当するアドレスが存在するとそのアドレスを利用して、今回の例の場合は１０．１０．１．１５に変換し、さらにデスティネーションのポート番号８０を、閉域網Ａ用に割り当てられたポート番号８０８０に変換され、そのパケットは該当するサーバへと運ばれる。もし、該当するアドレスがない場合は前述の方法によりサーバ側ネットワークにおいて割り当てられ、以下通常の場合と同様に通信が行われる。

【００４２】もし、仮にＤＮＳサーバ２に接続したいサーバのアドレスが登録されていない場合、ＤＮＳサーバ２はサーバ側ネットワークのＤＮＳサーバであるＤＮＳサーバ１にサーバのアドレスを問い合わせる。この問い合わせパケットはルーティングによりＡＳ１を経由してサーバ側ネットワークのＲＮＡＴ装置に送られる。受け取ったＲＮＡＴ装置は、パケットのソースとデスティネーションアドレスの両方を変換表に基づき変換する。そして、該当パケットがＤＮＳのアドレス問い合わせパケットの場合、パケットのデータには変更を加えずＤＮＳサーバ１へ送る。ＤＮＳサーバ１は、指定された接続先のサーバのアドレスをレスポンスとして返す。今回の場合、サーバのアドレス１０．１００．１０．１がデータとして埋め込まれる。このレスポンスパケットは、サーバ側ネットワークのルーティングによりＲＮＡＴ装置へと送られる。受け取ったＲＮＡＴ装置はデスティネーションアドレス１０．１０．１．６２（サーバ側ネットワークにおいて閉域網ＡのＤＮＳサーバ１に静的に割り当てたアドレス）からパケットが閉域網ＡのＡＳ１から来ているＰＰＰ回線１に送り出せばよいことを識別し、閉域網Ａに関する変換により正しくソースとデスティネーションアドレスを変換する。また、このパケットがＤＮＳのレスポンスパケットでありホストのアドレスを返すものである場合、データとして埋め込まれたサーバのアドレス１０．１００．１０．１を閉域網Ａにおいて割り当てられたサーバのアドレスである１０．１．１．１．に変換され、このパケットはＤＮＳサーバ２へと送られる。これを受け取ったＤＮＳサーバ２は、１０．１．１．１を接続したいサーバのアドレスとしてホスト１へ答え、ホスト１は通常の接続と同様にパケットを送出し通信を行う。

【００４３】逆にサーバ側ネットワーク上のＷＷＷサー

バが閉域網のホスト１に接続する場合について述べる。まず、サーバ側ネットワークのサーバがホスト１のアドレスをＤＮＳサーバ１に問い合わせる。ＤＮＳサーバ１はホスト１のアドレスを知らないので、ホスト１の名前に含まれているドメイン名などからホスト１がまず閉域網Ａに属するホストであることを認識する。そして、閉域網ＡのＤＮＳサーバであるＤＮＳサーバ２に対してサーバ側ネットワークで割り当てたアドレス（今回の場合、１０．１０．１．６２）をデスティネーションアドレスとしてアドレス問い合わせのパケットを送出する。このパケットはサーバ側のネットワークにおいてＲＮＡＴ装置へとルーティングされる。パケットを受け取ったＲＮＡＴ装置はデスティネーションアドレスから閉域網ＡのＰＰＰ回線１向けのパケットであることを識別し、閉域網Ａのアドレス空間へとソースとデスティネーションアドレスの両方を自身の持つ変換表により変換する。そして、閉域網ＡのＤＮＳサーバ２へと送出される。

【００４４】このパケットを受け取ったＤＮＳサーバ２は、問い合わせられているホスト１の閉域網Ａでのアドレス１０．０．１．１３をレスポンスとして、サーバ側ネットワークのＤＮＳサーバ１へと送る。このパケットはサーバ側ネットワークのＲＮＡＴ装置が受け取り、まずソースとデスティネーションアドレスを各々変換表より変換する。そして、このパケットがホストのアドレス問い合わせの答えであることからデータに埋め込まれているホストのアドレス部分をサーバ側ネットワークのアドレスへと変換する。この時、ＲＮＡＴ装置の持つ変換表を検索し該当するデータがあれば、変換表から対応するアドレスへと変換して、ＤＮＳサーバ１へ送る。また、該当するデータがない場合は、前述の方法によりホスト１へ閉域網ＡのＰＰＰ回線１用に割り当てたアドレス空間から動的にアドレスを割り当て、割り当てたアドレスへＤＮＳサーバ２からのレスポンスであるホスト１のアドレスを変更し、ＤＮＳサーバ１へ送る。今回は、アドレス１０．１０．１．１５が割り当てられ変換されることになる。この時、ＲＮＡＴ装置の持つ変換表に該当するホスト１に関するアドレスデータを付加する。このようにＤＮＳサーバのレスポンスであるホストのアドレスは変換され、変換されたアドレスが該当する閉域網のホストに接続要求しているサーバへと通知される。そして、通知されたアドレスをデスティネーションアドレスとして、サーバは閉域網に属するホストへの接続を試み、ＲＮＡＴによるアドレス変換機能によりサーバ側からホストへの接続が確立されて通信が開始される。

【００４５】このようにすることでＤＮＳサーバとの連携が可能であり、既存のＤＮＳサーバに変更を加える必要がなく利用が可能となり、多くの通信に利用されているＩＰネットワークでの導入が容易であり、またサーバと閉域網のホストの双方向からの接続の確立が実現できる。また、ＤＮＳサーバを利用してアドレスの通知を制

限すればサーバからの接続ができる閉域網のホストを限定するなど細かな制御も出来、閉域網の方針による閉域性の維持ができる。

【００４６】以上から、サーバ側のネットワークにおいて各閉域網毎にアドレス空間を用意し、さらには、各閉域網ごとにサーバに対して利用できるポート番号を決めて、受けとった／送り出すパケットの該当する各部分を変換しているので、サーバ側から端末への情報配信や閉域網毎、あるいは、地域毎にカスタマイズしたサービスの実現が可能になる。さらに閉域網単位にアドレスを割り当てるので閉域網の持つ閉域性を保持したまま複数閉域網に対し１台のサーバによるサービスの提供ができる仮想プライベートサーバの構築を可能にする。また、動的に割り当てるアドレスの割り当て有効期限をある一定時間／あるイベント終了までとすることで、一度動的に割り当てたアドレスの再利用が可能でありスケーラビリティやセキュリティを確保することも可能である。

第２発明の具体例

第１発明の具体例の場合と同様に、企業１が企業Ａ，Ｂに対して調達を行う場合を例にして述べる。ネットワークの構成は、図１５に示すようなものとなっている。即ち閉域網Ａ，Ｂ，１はそれぞれアクセスサーバＡＳ１，ＡＳ２，ＡＳ３によりインターネットと接続されサーバ側ネットワークはＶＮＡＴ機能付きアクセスサーバによりインターネットと接続されている。閉域網Ｎは、企業Ｎの持つ閉域網を示している。また、ＶＮＡＴ機能を持つ装置においては図１６に基づき各閉域網のＰＰＰ回線単位にＶＬＡＮタグを割り当てる。ホスト１がサーバ側ネットワーク上のサーバを利用する時、ＡＳ１とＶＮＡＴ機能付ＡＳ（以下、ＶＮＡＴ装置）との間にＰＰＰ接続がなければＰＰＰ接続を確立する。このＰＰＰ接続確立時の認証において、このＰＰＰ回線が閉域網ＡのＰＰＰ回線１であることが認証される。閉域網Ａを示すＶＮＡＴタグとしてＶＬＡＮ１が割り当てられており、これまでＰＰＰ回線１を示すために子番号を用いてこのＰＰＰ回線１に対してＶＮＡＴ１－１というＶＬＡＮタグが割り当てられる。これにより、閉域網ＡのＰＰＰ回線１であることを識別できる。ＰＰＰ回線２が確立した場合は、ＶＬＡＮ１－２というように子番号をＰＰＰ回線に対応させるものとする。ＶＬＡＮタグの形式は既存のＶＬＡＮ技術を利用するために、ＩＥＥＥ８０２．１０などで定義されているものなど既存のものを用い、情報量としてここに述べたどの閉域網のどのＰＰＰ回線であるか識別できるものであればよい。

【００４７】ＶＮＡＴ機能によりこのＰＰＰ回線を通してサーバ側のネットワークに来るパケットに関しては、図９に示したようにＶＬＡＮタグを埋め込み、このタグを基にサーバへ配送される。そして、サーバではＶＬＡＮタグ毎に様々な処理を行うプログラム、例えばＯＳを別個に動作させ処理を行う。このサーバではＶＬＡＮタ

グと接続してきたホストの情報を関連付けることでホストへ向けてパケットの送出時には、適切なＶＬＡＮタグをつけて送り出すことができる。これにより、サーバ側ネットワークでのアドレスの変換は必要とすることなく、自閉域網に存在するかのようにサーバを利用できる。また、ＶＬＡＮタグ毎にＯＳが動作しているためにその動作は閉域網単位で柔軟に変更できるようになっており、参照・登録するデータもＶＬＡＮタグをキーにして制限をかけることができる。サーバ側ネットワークから閉域網へ送り出される時には、受け取ったパケットについているＶＬＡＮタグを取り除き、ＶＬＡＮタグからパケットの配送先として適切な閉域網と適切なＰＰＰ回線を識別し正しいＰＰＰ回線へと送り出す。

【００４８】ホスト２がサーバ側のネットワークに接続する場合は、ＰＰＰ回線２を利用するので、このホスト２からサーバ側ネットワークへのパケットには前述の方法と同様にＶＬＡＮタグが割り当てられＶＬＡＮ１－２を用いることになる。このタグを用いて、ホスト１の場合と同様に動作する。各々のパケットに埋め込まれるＶＬＡＮタグは異なるが、サーバは閉域網Ａを示すＶＬＡＮ１を基にして動作を決定するので、利用するＰＰＰ回線が異なっていても同一のデータを参照・変更できる。逆に、サーバからホスト１，２へのパケットはＶＬＡＮタグにより閉域網Ａへのものであることが識別され、さらにＶＬＡＮタグの子番号を基にホスト１へのパケットはＰＰＰ回線１へ、ホスト２へのパケットはＰＰＰ回線２へと適切に振り分けられる。

【００４９】ホスト３，４は同じＡＳ２を介してサーバ側ネットワークに接続しており、ともにＰＰＰ回線１を利用しているので、利用するＶＬＡＮタグは同じでＶＬＡＮ２－１を用いて、ＶＮＡＴ装置においてパケットに組み込まれ、サーバへと送られる。サーバからホストへのパケットも前述のホスト１と同様にして適切なＰＰＰ回線を通りホストへと送られる。

【００５０】ホスト５の場合も同様に、ＰＰＰ接続確立時に所属する閉域網が閉域網１であり、これがＰＰＰ回線１であることが認証され、それに基づき閉域網１を示すＶＬＡＮタグであるＶＬＡＮ３、ＰＰＰ回線１を示すＶＬＡＮタグであるＶＬＡＮ３－１が割り当てられる。そして、他のホスト同様の動作により正しくホストとサーバ間においてやり取りされる。また、ＶＬＡＮタグがＶＬＡＮ３に関する処理をするＯＳからは、ＶＬＡＮタグがＶＬＡＮ１，ＶＬＡＮ２しか参照できないデータを参照することが出来るようにすることで、企業１のユーザは、企業Ａ，Ｂが登録したデータを見ることができ、今回の例となっている調達業務に必要となる制限付きの閉域網間の通信が実現される。

【００５１】次に、ＩＰネットワークによる通信時に重要な動きをするＤＮＳ（Domain Name System）サーバとの動きであるが、第２発明の場合はサーバは確かにサーバ側のネットワーク上にあるが、ＶＬＡＮ機能の利用により仮想的に閉域網内での通信が実現されているので、ＤＮＳサーバは通常の場合と同様の利用が可能であり、サーバに割り当てられたアドレス宛のパケットが正しく閉域網においてサーバ側のネットワークにあるＶＮＡＴ装置とＰＰＰ接続できるＡＳへと正しくルーティングされるように設定するだけで利用が可能になる。

【００５２】このようにして、サーバのアドレスをデスティネーションアドレスとし、そのパケットがサーバ側ネットワークへ運ばれるようにするなど、ユーザ側のネットワークに変更を最小限にしてサーバ側の制御のもと１台のサーバにより複数の閉域網に対して各々サーバがあるかのように動作できる仮想プライベートサーバによるサービスの提供が可能になる。

【００５３】第２発明の変形に対する具体例を以下に示す。ＰＰＰ回線確立時に所属する閉域網の認証を行い、閉域網単位で、ＰＰＰ回線と受けとったパケットの送出元であるホストのアドレスとを対応付ける。今回の場合、図１７に示すような表をＶＮＡＴ装置が持つことになる。また各閉域網Ａ，Ｂ…に対してＶＬＡＮタグ，ＶＬＡＮ１，ＶＬＡＮ２，…が予め割り当てられてある。

【００５４】ホスト１がサーバ側ネットワークに接続を試みると、ＡＳ１とＶＮＡＴ装置との間にＰＰＰ回線１が確立され、閉域網Ａであることが認証される。そして、この認証結果によりＶＬＡＮタグのＶＬＡＮ１がこのＰＰＰ回線１に割り当てられる。そして、ホスト１からのパケットがＶＮＡＴ装置に到着すると、ＶＮＡＴ装置ではパケットに埋め込まれたホスト１のアドレス１０．０．１．１３と、パケットが運ばれてきたＰＰＰ回線１とを対応付ける。そして、認証結果により割り当てられたＶＬＡＮタグを埋め込み、サーバへと送られる。逆に、サーバからパケットが到着すると、埋め込まれたＶＬＡＮタグのＶＬＡＮ１により図１７の対応表からＶＬＡＮ１に関するものを選択し、パケットのデスティネーションアドレスであるホスト１のアドレス１０．０．１．１３をキーにして検索を行い、対応表よりこのパケットを閉域網Ａとの間に確立されたＰＰＰ回線１に送り出せばよいことを認識し、ＶＬＡＮタグを取り除きＰＰＰ回線１へと送り出す。このようにして、同一の閉域網から複数のＰＰＰ回線が確立された場合でも、パケットを受けとったＰＰＰ回線へ正しくパケットを送り出すことができる。

【００５５】ホスト２の場合は、閉域網Ａに属するホストであるので、ホスト１と同様にＶＬＡＮ１が割り当てられる。しかし、利用しているＰＰＰ回線がホスト１と異なるので、ホスト２のアドレス１０．０．３．２０はＰＰＰ回線２へと対応付けされる。これにより、ホスト１と同様にＶＬＡＮ１がパケットに埋め込まれるが、サーバからのパケットはこの対応表により、ホスト２宛のパケットは適切にＰＰＰ回線２を利用して送られる。ホ

スト３，４，５の場合も同様の方法によりＶＬＡＮタグが割り当てられ、ホストのアドレスとＰＰＰ回線が割り当てられ、ＶＬＡＮタグ単位で独立して管理される。これにより、適切な閉域網の適切なＰＰＰ回線へとパケットを送り出すことができる。

【００５６】次に図１８を参照して図１中のＲ－ＮＡＴ装置、つまりルートサイドＮＡＴ機能付きアクセスサーバの概略機能構成を説明する。複数のＰＰＰ回線処理部１１が設けられＰＰＰ回線処理部１１には認証部１２が付属されている。ＰＰＰ回線確立の際にどの閉域網のどのＰＰＰ回線であるかの認証が認証部１２で確認され、図２Ｂに示したアドレス割り当てテーブル１３を参照してそのＰＰＰ回線を利用して到着したパケットのホストにサーバ側ネットワークの割り当て分のうち空きアドレスが割り当てられ、その各閉域網のＰＰＰ回線と閉域網側のアドレスと、割り当てたサーバ側ネットワークのアドレスとの対応表（変換表）１４が作られる。ＰＰＰ回線処理部１１に端末からパケットが来ると、そのＰＰＰ回線が確立していれば、その閉域網とＰＰＰ回線に該当する対応表１４を参照して、そのパケットのアドレスに対して、アドレス変換部１５でアドレス変換を行ってサーバ側ネットワークへ送られる。サーバ側ネットワークからのパケットは、そのアドレスにより対応表１４を参照して、閉域網側で付与したアドレスに変換すると共にどの閉域網のどのＰＰＰ回線かを知り、対応するＰＰＰ回線処理部１１よりＰＰＰ回線へ送出する。

【００５７】このＲ－ＮＡＴ装置において閉域網からパケットに対する処理は図１９に示すようになる。まず最初のパケットの到来に先立ち、ＰＰＰ回線接続要求があるかがＰＰＰ回線処理部１１で調べられ（Ｓ１）、接続要求であればどの閉域網のどのＰＰＰ回線からの要求であるかを認証し（Ｓ２）、ＰＰＰ回線を確立する（Ｓ３）。

【００５８】この状態でそのＰＰＰ回線を利用したホストからのパケットを待ち（Ｓ４）、パケットが到来すると、その閉域網とソースアドレスにより対応表１４を検索し（Ｓ５）、対応するものがなければ、そのパケットのアドレスに対し、アドレス割り当てテーブル１３を参照してサーバ側ネットワークのアドレスを割り当て、これらの関係を対応表１４に書込む（Ｓ６）。到来パケットについてそのアドレスで対応表１４を検索し、アドレス変換部１５でアドレス変換してサーバ側ネットワークへ送る（Ｓ７）。その後に到来するパケットはＰＰＰ回線が確立されているから、ステップＳ４のパケット待ち状態にあり、また対応表１４の検索によりアドレスが見つかる場合は（Ｓ５）、対応表（変換表）１４にもとづくアドレス変換を行ってサーバ側ネットワークへ送出する（Ｓ７）。見つからない場合は、上記のようにアドレス割り当て対応表１４を作成する。

【００５９】次に図８中のＶＮＡＴ装置（ＶＮＡＴ機能

付きアクセスサーバ）の概略機能構成を図２０を参照して説明する。図１８の場合と同様に複数のＰＰＰ回線確立部１１、これに付属する認証部１２が設けられ、ＰＰＰ回線確立時に、どの閉域網のどのＰＰＰ回線かが認識され、そのＰＰＰ回線には図９に示すようなＶＬＡＮタグテーブル２１によりその閉域網のそのＰＰＰ回線と対応したＶＬＡＮタグが割り当てられる。そのＰＰＰ回線を通じて到来したパケットに対し、パケット変換部２２で、そのＰＰＰ回線に割り当てられたＶＬＡＮタグが付加されて、サーバ側ネットワークへ送出される。

【００６０】サーバ側ネットワークから到来したパケットは、パケット変換部２２でそのＶＬＡＮタグによりＶＬＡＮタグテーブル２１を検索し、対応するＰＰＰ回線へ、ＶＬＡＮタグを除去して送出する。このＶＮＡＴ装置における閉域網からのパケットに対する処理は図２１に示すようになる。まず最初のパケットの到来に先立ち、ＰＰＰ回線接続要求があり（Ｓ１）、どの閉域網のどのＰＰＰ回線からの要求であるかの認証を行い（Ｓ２）、ＰＰＰ回線を確立する（Ｓ３）。

【００６１】その後、その確立したＰＰＰ回線にパケットが到来すると（Ｓ４）、その閉域網のそのＰＰＰ回線でＶＬＡＮタグテーブル２１を検索して該当するＶＬＡＮタグを取出し（Ｓ５）、これをパケット変換部２２でパケットに埋込みサーバ側ネットワークへ送る（Ｓ６）。ＶＬＡＮタグとして、ＰＰＰ回線を区別する番号を用いない、図１２や図１７を参照して説明した場合においてはＶＮＡＴ装置は図２０中のＶＬＡＮタグテーブル２１が閉域網とＶＬＡＮタグとの対応を示すものとなり、更に図２０中に破線で示すようにＰＰＰ回線が確立され、埋込むＶＬＡＮタグが決まると、図１２又は図１７に示すような、そのＶＬＡＮタグとそのＰＰＰ回線と、そのパケットの閉域網の（ソース）アドレスとの関係を示す対応表２３を作成する。サーバ側ネットワークからのパケットは、そのＶＬＡＮタグと、その（デスティネーション）アドレスとにより対応表２３を参照してパケット変換部２２でどの閉域網のどのＰＰＰ回線へ、ＶＬＡＮタグを除去したパケットを送るかを決定する。

【００６２】図２１に示した処理においては、ステップＳ６の代りに破線で示すようにＶＬＡＮタグを埋込み送出すると共にＶＬＡＮタグと、到来したＰＰＰ回線と（ソース）アドレスとの対応表を作成することになり、その他は同様である。上述では複数閉域網間の通信にこの発明を適用したが、複数ユーザ側ネットワークとサーバ側ネットワークとの通信にもこの発明は適用できる。

【００６３】

【発明の効果】この発明では、ＰＰＰ接続により各閉域網がサーバ側のネットワークに接続され、このＰＰＰ接続確立時に所属する閉域網とＰＰＰ回線自体を認証することにより、閉域網単位に割り当てたアドレス空間により様々な制御がサーバ側で容易に行える。これにより、

27

複数の閉域網のユーザ端末に対し、閉域性を失うことなく各閉域網にカスタマイズした共通サービスの提供を物理的に１台のサーバにより可能にし、各閉域網からは自閉域網に各々サーバが存在するように利用できる。また、今後増えゆくと予想される複数企業間でのデータ交換を必要とするプロジェクトの実施時や調達業務の実施時に必要となる複数閉域網向けの共用サーバの構築、運用などを提供するハウジングサービスが展開できる。このサービスを利用することで、ユーザは自社の閉域網を変更せず、また、閉域性を失う事なく容易にプロジェクト毎に一時的に必要となる共用サーバの運用ができ、複数の企業と連携して行うプロジェクトの情報化がスムーズに行えるので、この発明により実現されるサービスは、現在ＩＳＰ（Internet Service Provider ）が行っているＶＰＮ（Virtual Private Network)サービスの新しい付加サービスとしての展開が見込める。また、この方法により実現されるサーバ側から閉域網のホストへの閉域性を維持しての接続確立が可能であることを利用して、サーバ側ネットワークに複数の閉域網で提供されている種々のサービスを統合的に利用できるサーバを構築し、個人向けのポータルサイトサービスの展開も可能になる。このように、この発明は閉域網向けの新しい情報流通プラットフォームを構築する手段としての利用が見込める。

【図面の簡単な説明】

【図１】第１発明を適用したシステムの構成例を示す図。

【図２】Ａは図１中のＲ－ＮＡＴにおけるアドレス変換テーブルの例を示す図、Ｂは各閉域網に対する、サーバ側ネットワークのアドレス空間の割り当て例を示す図である。

【図３】ホスト１についてのパケットの変換の様子を示す図。

【図４】ネットワークアドレス変換のイメージを示す図。

28

*【図５】閉域網に割り当てられたネットワークアドレス空間の利用方針を示す図。

【図６】パケットにおけるアドレス変換の様子を示す図。

【図７】第１発明と従来技術との特徴の関係を示す図。

【図８】第２発明を適用したシステムの構成例を示す図。

【図９】ＶＬＡＮタグの割り当て例を示す図。

【図１０】ＶＮＡＴ機能のパケットに対する動作を示す図。

【図１１】ＶＮＡＴタグを利用したサーバ内の動作を示す図。

【図１２】第２発明におけるＶＬＡＮタグの対応付けの例を示す図。

【図１３】第１発明の具体例におけるシステムを示す図。

【図１４】図１２中のＲ－ＮＡＴ装置でのアドレス割り当ての例を示す図。

【図１５】第２発明の具体例におけるシステムを示す図。

【図１６】図１５中のＶＮＡＴ装置におけるＶＬＡＮタグの割り当て例を示す図。

【図１７】第２発明の変形におけるＶＬＡＮタグとアドレスとＰＰＰ回線の対応を示す図。

【図１８】Ｒ－ＮＡＴ装置の概略機能構成を示す図。

【図１９】Ｒ－ＮＡＴ装置における処理の一部を示す流れ図。

【図２０】Ｖ－ＮＡＴ装置の概略機能構成を示す図。

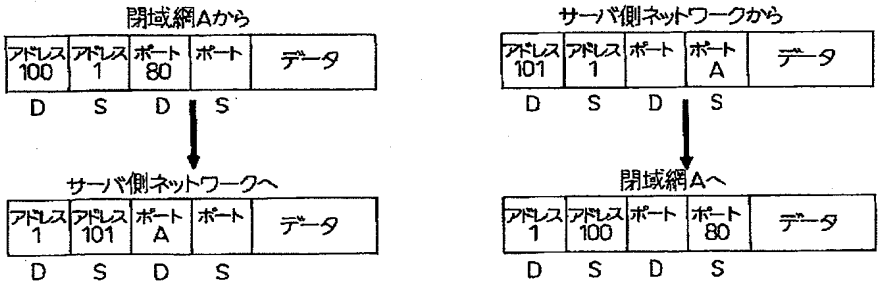
【図２１】Ｖ－ＮＡＴ装置における処理の一部を示す流れ図。

【図２２】従来のＰＰＰトンネリング接続のシステムを示す図。

【図２３】従来のＮＡＴによる接続のシステムを示す図。

*

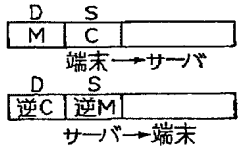
【図３】



S:ソース
D:デスティネーション

図3

【図６】



S:ソース
D:デスティネーション
C:Compaction変換
M:Merge変換

図6

【図１】

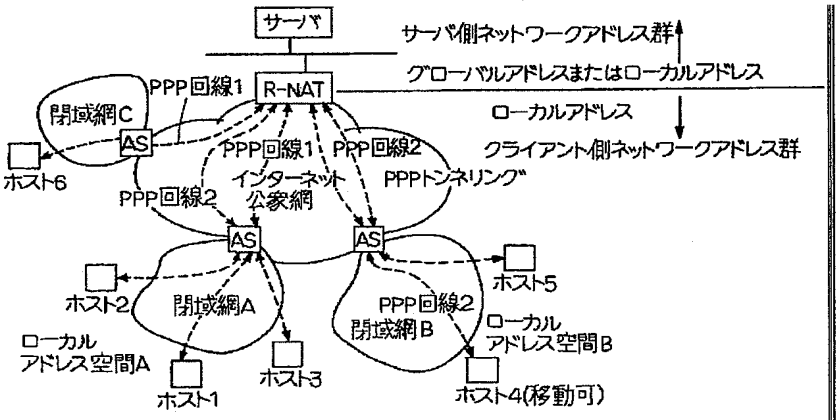


図１

【図１１】

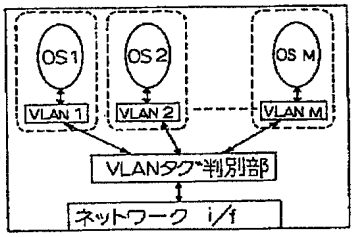


図11

【図２】

A

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト１	アドレス１	—	アドレス 101
ホスト２	アドレス２	—	アドレス 220
ホスト３	アドレス３	—	アドレス 102
ホスト４	—	アドレス 11	アドレス 301（静的）
ホスト５	—	アドレス 22	アドレス 321
Server	アドレス100	アドレス 150	アドレス１

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間 101-300	アドレス空間 301-350
PPP回線１	アドレス空間 101-200	アドレス空間 311-350
PPP回線２	アドレス空間 201-250	アドレス 301
動的割り当て	アドレス空間 251-300	—

図２

【図５】

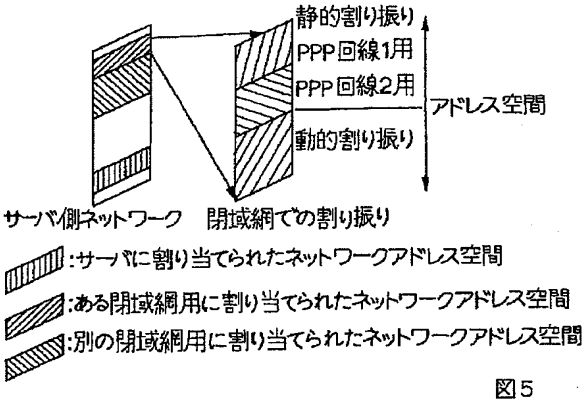


図５

【図１６】

	閉域網 A	閉域網 B	閉域網 1
PPP回線１	VLAN 1-1	VLAN 2-1	VLAN 3-1
PPP回線２	VLAN 1-2	—	—

図１６

【図７】

	従来のNAT	PPP トンネリング	方法１ (Root-side NAT)
ローカルアドレスの使用	○	○	○
サーバープッシュ型情報配信	×	×	○
カスタマイズドサービスの提供	△	×	○
不正アクセスパスの発生防止	×	×	○

図７

【図４】

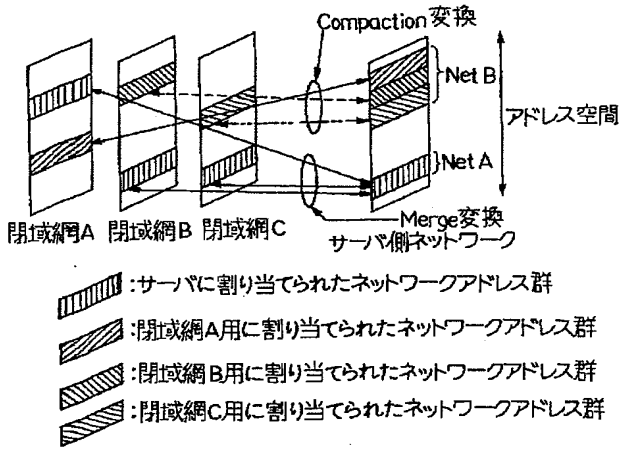
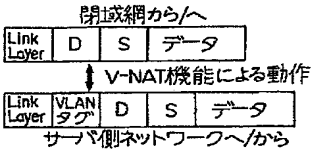


図4

【図１０】



S:ソースネットワークアドレス
D:デスティネーションネットワークアドレス

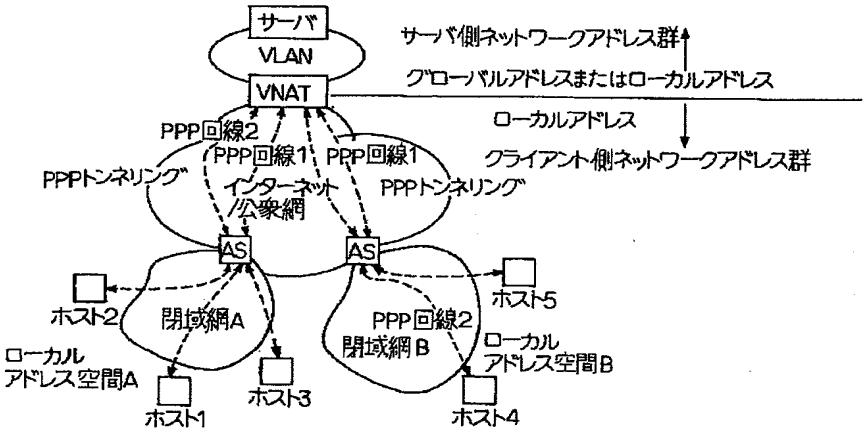
図10

【図１７】

VLANタグ	アドレス	PPP回線番号
VLAN 1	10. 0. 1. 13	PPP回線１
VLAN 1	10. 0. 3. 20	PPP回線２
VLAN 2	10. 0. 1. 30	PPP回線１
VLAN 2	10. 0. 1. 14	PPP回線１
VLAN 3	10. 1. 1. 1	PPP回線１

図17

【図８】



VNAT:VNAT機能付きアクセスサーバ
AS:アクセスサーバ

図8

【図９】

	閉域網 A	閉域網 B	VLANタグ
ホスト１	アドレス１	—	VLAN 1-1
ホスト２	アドレス２	—	VLAN 1-2
ホスト３	アドレス３	—	VLAN 1-1
ホスト４	—	アドレス 11	VLAN 2-2
ホスト５	—	アドレス 22	VLAN 2-1
Server	アドレス100	アドレス 150	アドレス１

図9

【図１２】

VLANタグ	ホストのアドレス	PPP回線番号
VLAN1	アドレス1	PPP回線1
VLAN1	アドレス2	PPP回線2
VLAN1	アドレス3	PPP回線1
VLANタグ	ホストのアドレス	PPP回線番号
VLAN2	アドレス4	PPP回線2
VLAN2	アドレス5	PPP回線1

図12

【図１３】

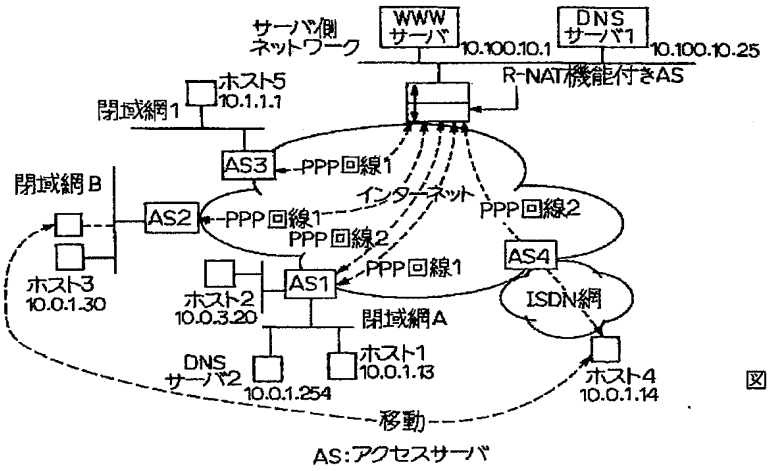


図13

【図１４】

	閉域網 A	閉域網 B	閉域網 1	サーバ側ネットワーク
ホスト 1	10. 0. 1. 13	—	—	10. 10. 1. 15
ホスト 2	10. 0. 3. 20	—	—	10. 10. 1. 100
ホスト 3	—	10. 0. 1. 30	—	10. 10. 2. 10
ホスト 4	—	10. 0. 1. 14	—	10. 10. 2. 65
ホスト 5	—	—	10. 1. 1. 1	10. 10. 11. 1
Server	10. 1. 1. 1	10. 10. 15. 1	10. 50. 1. 1	10. 100. 10. 1

図１４

【図２２】

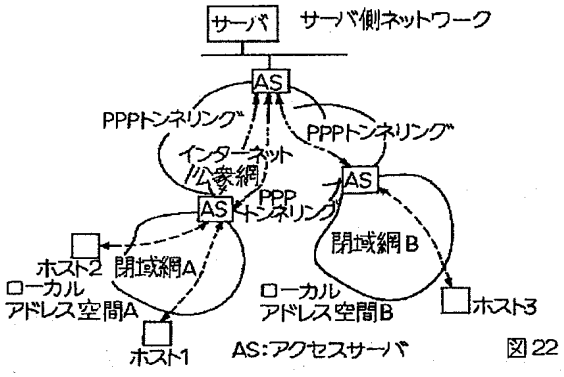


図22

【図１５】

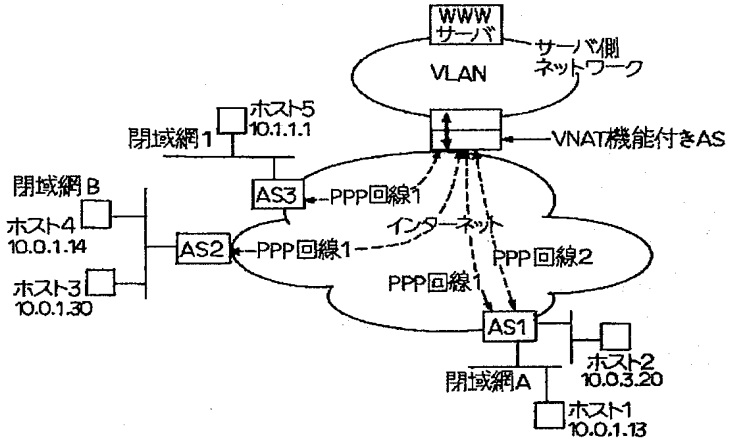


図15

【図１８】

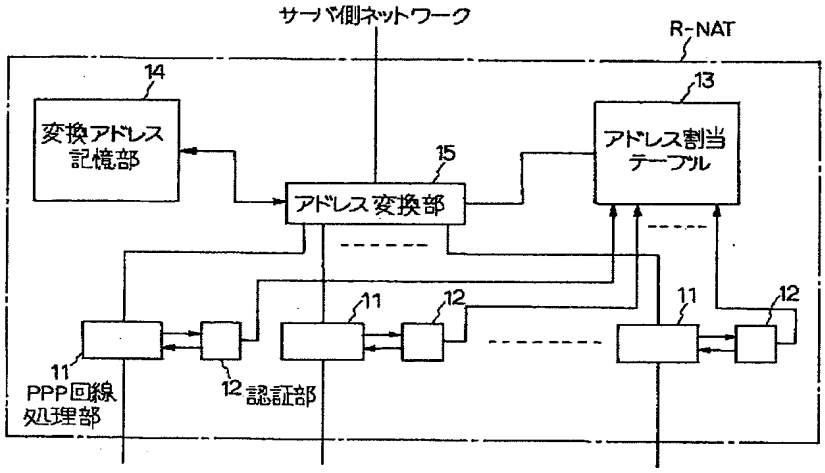


図18

【図１９】

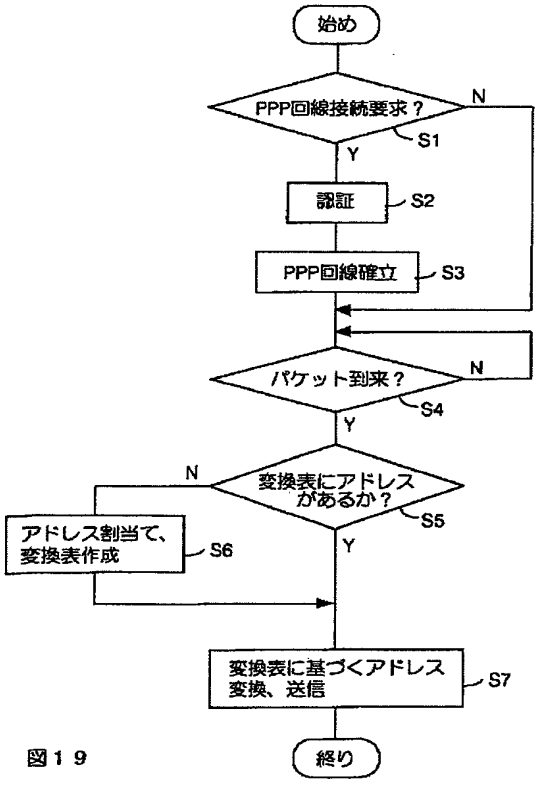


図１９

【図２１】

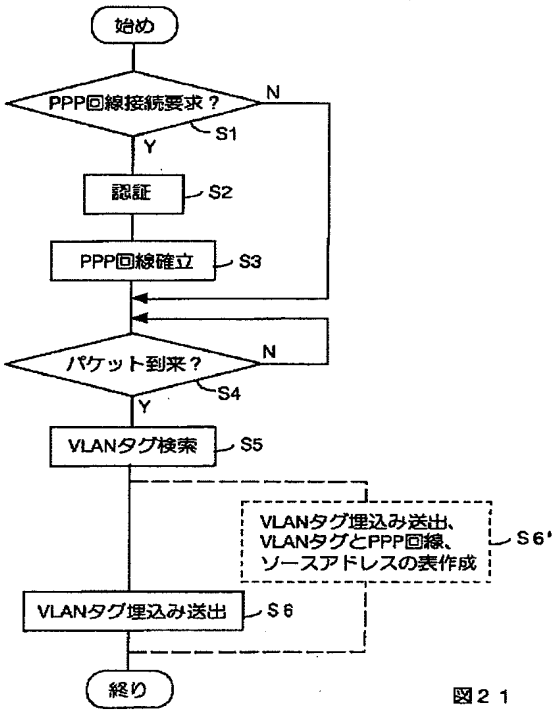


図２１

【図２０】

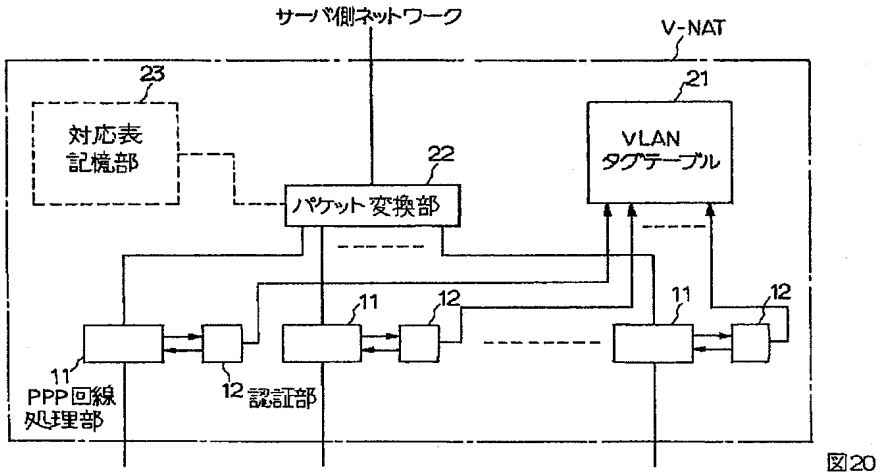


図20

【図２３】

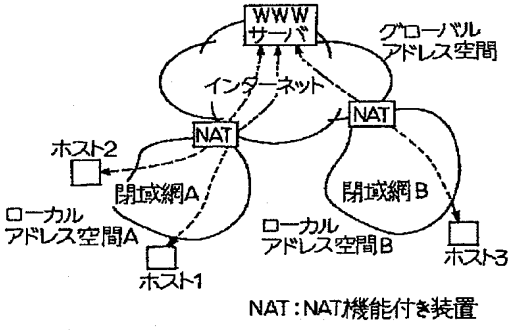


図23